112TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
112–264

CYBERSECURITY ENHANCEMENT ACT OF 2011

OCTOBER 31, 2011.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. HALL, from the Committee on Science, Space, and Technology, submitted the following

R E P O R T

[To accompany H.R. 2096]

[Including cost estimate of the Congressional Budget Office]

The Committee on Science, Space, and Technology, to whom was referred the bill (H.R. 2096) to advance cybersecurity research, development, and technical standards, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

I. AMENDMENT

The amendment is as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity Enhancement Act of 2011".

TITLE I—RESEARCH AND DEVELOPMENT

SEC. 101. DEFINITIONS.

In this title:

(1) NATIONAL COORDINATION OFFICE.—The term National Coordination Office means the National Coordination Office for the Networking and Information Technology Research and Development program.

(2) PROGRAM.—The term Program means the Networking and Information Technology Research and Development program which has been established under section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511).

SEC. 102. FINDINGS.

Section 2 of the Cyber Security Research and Development Act (15 U.S.C. 7401) is amended—

(1) by amending paragraph (1) to read as follows:

"(1) Advancements in information and communications technology have resulted in a globally interconnected network of government, commercial, scientific, and education infrastructures, including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services.";

(2) in paragraph (2), by striking "Exponential increases in interconnectivity have facilitated enhanced communications, economic growth," and inserting "These advancements have significantly contributed to the growth of the United States economy";

(3) by amending paragraph (3) to read as follows:

"(3) The Cyberspace Policy Review published by the President in May, 2009, concluded that our information technology and communications infrastructure is vulnerable and has 'suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information'."; and

(4) by amending paragraph (6) to read as follows:

"(6) While African-Americans, Hispanics, and Native Americans constitute 33 percent of the college-age population, members of these minorities comprise less than 20 percent of bachelor degree recipients in the field of computer sciences.".

SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DEVELOPMENT PLAN.

(a) IN GENERAL.—Not later than 12 months after the date of enactment of this Act, the agencies identified in subsection 101(a)(3)(B)(i) through (x) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)(i) through (x)) or designated under section 101(a)(3)(B)(xi) of such Act, working through the National Science and Technology Council and with the assistance of the National Coordination Office, shall transmit to Congress a strategic plan based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking systems. Once every 3 years after the initial strategic plan is transmitted to Congress under this section, such agencies shall prepare and transmit to Congress an update of such plan.

(b) CONTENTS OF PLAN.—The strategic plan required under subsection (a) shall—

(1) specify and prioritize near-term, mid-term and long-term research objectives, including objectives associated with the research areas identified in section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) and how the near-term objectives complement research and development areas in which the private sector is actively engaged;

(2) describe how the Program will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure, and to protect consumer privacy;

(3) describe how the Program will foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the

timely benefit of society and the national interest, including through the dissemination of best practices and other outreach activities;

(4) describe how the Program will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems;

(5) describe how the Program will facilitate access by academic researchers to the infrastructure described in paragraph (4), as well as to relevant data, including event data; and

(6) describe how the Program will engage females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b) to foster a more diverse workforce in this area.

(c) DEVELOPMENT OF ROADMAP.—The agencies described in subsection (a) shall develop and annually update an implementation roadmap for the strategic plan required in this section. Such roadmap shall—

(1) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated;

(2) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

(3) estimate the funding required for each major research objective of the strategic plan for the following 3 fiscal years.

(d) RECOMMENDATIONS.—In developing and updating the strategic plan under subsection (a), the agencies involved shall solicit recommendations and advice from—

(1) the advisory committee established under section 101(b)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)(1)); and

(2) a wide range of stakeholders, including industry, academia, including representatives of minority serving institutions and community colleges, National Laboratories, and other relevant organizations and institutions.

(e) APPENDING TO REPORT.—The implementation roadmap required under subsection (c), and its annual updates, shall be appended to the report required under section 101(a)(2)(D) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)(D)).

SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSECURITY.

Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) by inserting "and usability" after "to the structure";

(2) in subparagraph (H), by striking "and" after the semicolon;

(3) in subparagraph (I), by striking the period at the end and inserting "; and"; and

(4) by adding at the end the following new subparagraph:

"(J) social and behavioral factors, including human-computer interactions, usability, and user motivations.".

SEC. 105. NATIONAL SCIENCE FOUNDATION CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY RESEARCH AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (A) by inserting "identity management," after "cryptography,"; and

(2) in subparagraph (I), by inserting ", crimes against children, and organized crime" after "intellectual property".

(b) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—Section 4(a)(3) of such Act (15 U.S.C. 7403(a)(3)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $90,000,000 for fiscal year 2012;

"(B) $90,000,000 for fiscal year 2013; and

"(C) $90,000,000 for fiscal year 2014.".

(c) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—Section 4(b) of such Act (15 U.S.C. 7403(b)) is amended—

(1) in paragraph (4)—

(A) in subparagraph (C), by striking "and" after the semicolon;

(B) in subparagraph (D), by striking the period and inserting "; and"; and

(C) by adding at the end the following new subparagraph:

"(E) how the center will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions."; and

(2) in paragraph (7) by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $4,500,000 for fiscal year 2012;
"(B) $4,500,000 for fiscal year 2013; and
"(C) $4,500,000 for fiscal year 2014.".

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of such Act (15 U.S.C. 7404(a)(6)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $19,000,000 for fiscal year 2012;
"(B) $19,000,000 for fiscal year 2013; and
"(C) $19,000,000 for fiscal year 2014.".

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of such Act (15 U.S.C. 7404(b)(2)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $2,500,000 for fiscal year 2012;
"(B) $2,500,000 for fiscal year 2013; and
"(C) $2,500,000 for fiscal year 2014.".

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY.—Section 5(c)(7) of such Act (15 U.S.C. 7404(c)(7)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $24,000,000 for fiscal year 2012;
"(B) $24,000,000 for fiscal year 2013; and
"(C) $24,000,000 for fiscal year 2014.".

(g) CYBER SECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—Section 5(e) of such Act (15 U.S.C. 7404(e)) is repealed.

SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation shall continue a Scholarship for Service program under section 5(a) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)) to recruit and train the next generation of Federal cybersecurity professionals and to increase the capacity of the higher education system to produce an information technology workforce with the skills necessary to enhance the security of the Nation's communications and information infrastructure.

(b) CHARACTERISTICS OF PROGRAM.—The program under this section shall—

(1) provide, through qualified institutions of higher education, scholarships that provide tuition, fees, and a competitive stipend for up to 2 years to students pursing a bachelor's or master's degree and up to 3 years to students pursuing a doctoral degree in a cybersecurity field;

(2) provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal information technology workforce; and

(3) increase the capacity of institutions of higher education throughout all regions of the United States to produce highly qualified cybersecurity professionals, through the award of competitive, merit-reviewed grants that support such activities as—

(A) faculty professional development, including technical, hands-on experiences in the private sector or government, workshops, seminars, conferences, and other professional development opportunities that will result in improved instructional capabilities;

(B) institutional partnerships, including minority serving institutions and community colleges; and

(C) development of cybersecurity-related courses and curricula.

(c) SCHOLARSHIP REQUIREMENTS.—

(1) ELIGIBILITY.—Scholarships under this section shall be available only to students who—

(A) are citizens or permanent residents of the United States;

(B) are full-time students in an eligible degree program, as determined by the Director, that is focused on computer security or information assurance at an awardee institution; and

(C) accept the terms of a scholarship pursuant to this section.

(2) SELECTION.—Individuals shall be selected to receive scholarships primarily on the basis of academic merit, with consideration given to financial need, to the goal of promoting the participation of individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b), and to veterans. For purposes of this paragraph, the term "veteran" means a person who—

(A) served on active duty (other than active duty for training) in the Armed Forces of the United States for a period of more than 180 consecutive days, and who was discharged or released therefrom under conditions other than dishonorable; or

(B) served on active duty (other than active duty for training) in the Armed Forces of the United States and was discharged or released from such service for a service-connected disability before serving 180 consecutive days.

For purposes of subparagraph (B), the term "service-connected" has the meaning given such term under section 101 of title 38, United States Code.

(3) SERVICE OBLIGATION.—If an individual receives a scholarship under this section, as a condition of receiving such scholarship, the individual upon completion of their degree must serve as a cybersecurity professional within the Federal workforce for a period of time as provided in paragraph (5). If a scholarship recipient is not offered employment by a Federal agency or a federally funded research and development center, the service requirement can be satisfied at the Director's discretion by—

(A) serving as a cybersecurity professional in a State, local, or tribal government agency; or

(B) teaching cybersecurity courses at an institution of higher education.

(4) CONDITIONS OF SUPPORT.—As a condition of acceptance of a scholarship under this section, a recipient shall agree to provide the awardee institution with annual verifiable documentation of employment and up-to-date contact information.

(5) LENGTH OF SERVICE.—The length of service required in exchange for a scholarship under this subsection shall be 1 year more than the number of years for which the scholarship was received.

(d) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) GENERAL RULE.—If an individual who has received a scholarship under this section—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section; or

(E) fails to fulfill the service obligation of the individual under this section,

such individual shall be liable to the United States as provided in paragraph (3).

(2) MONITORING COMPLIANCE.—As a condition of participating in the program, a qualified institution of higher education receiving a grant under this section shall—

(A) enter into an agreement with the Director of the National Science Foundation to monitor the compliance of scholarship recipients with respect to their service obligation; and

(B) provide to the Director, on an annual basis, post-award employment information required under subsection (c)(4) for scholarship recipients through the completion of their service obligation.

(3) AMOUNT OF REPAYMENT.—

(A) LESS THAN ONE YEAR OF SERVICE.—If a circumstance described in paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(B) MORE THAN ONE YEAR OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(C) REPAYMENTS.—A loan described in subparagraph (A) or (B) shall be treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher Education Act of 1965 (20 U.S.C. 1087a and following), and shall be subject to repayment, together with interest thereon accruing from the date of the scholarship award, in accordance with terms and conditions specified by the Director (in consultation with the Secretary of Education) in regulations promulgated to carry out this paragraph.

(4) COLLECTION OF REPAYMENT.—

(A) IN GENERAL.—In the event that a scholarship recipient is required to repay the scholarship under this subsection, the institution providing the scholarship shall—

(i) be responsible for determining the repayment amounts and for notifying the recipient and the Director of the amount owed; and

(ii) collect such repayment amount within a period of time as determined under the agreement described in paragraph (2), or the repayment amount shall be treated as a loan in accordance with paragraph (3)(C).

(B) RETURNED TO TREASURY.—Except as provided in subparagraph (C) of this paragraph, any such repayment shall be returned to the Treasury of the United States.

(C) RETAIN PERCENTAGE.—An institution of higher education may retain a percentage of any repayment the institution collects under this paragraph to defray administrative costs associated with the collection. The Director shall establish a single, fixed percentage that will apply to all eligible entities.

(5) EXCEPTIONS.—The Director may provide for the partial or total waiver or suspension of any service or payment obligation by an individual under this section whenever compliance by the individual with the obligation is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(e) HIRING AUTHORITY.—For purposes of any law or regulation governing the appointment of individuals in the Federal civil service, upon successful completion of their degree, students receiving a scholarship under this section shall be hired under the authority provided for in section 213.3102(r) of title 5, Code of Federal Regulations, and be exempted from competitive service. Upon fulfillment of the service term, such individuals shall be converted to a competitive service position without competition if the individual meets the requirements for that position.

SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.

Not later than 180 days after the date of enactment of this Act the President shall transmit to the Congress a report addressing the cybersecurity workforce needs of the Federal Government. The report shall include—

(1) an examination of the current state of and the projected needs of the Federal cybersecurity workforce, including a comparison of the different agencies and departments, and an analysis of the capacity of such agencies and departments to meet those needs;

(2) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector, and a description of how successful programs are engaging the talents of females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b);

(3) an examination of the effectiveness of the National Centers of Academic Excellence in Information Assurance Education, the Centers of Academic Excellence in Research, and the Federal Cyber Scholarship for Service programs in promoting higher education and research in cybersecurity and information assurance and in producing a growing number of professionals with the necessary cybersecurity and information assurance expertise, including individuals from States or regions in which the unemployment rate exceeds the national average;

(4) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibilities; and

(5) recommendations for Federal policies to ensure an adequate, well-trained Federal cybersecurity workforce.

SEC. 108. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE.

(a) ESTABLISHMENT OF UNIVERSITY-INDUSTRY TASK FORCE.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall convene a task force to explore mechanisms for carrying out collaborative research, development, education, and training activities for cybersecurity through a consortium or other appropriate entity with participants from institutions of higher education and industry.

(b) FUNCTIONS.—The task force shall—

(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration;

(3) define the roles and responsibilities for the participants from institutions of higher education and industry in such entity;

(4) propose guidelines for assigning intellectual property rights, for the transfer of research and development results to the private sector; and

(5) make recommendations for how such entity could be funded from Federal, State, and nongovernmental sources.

(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education, including minority-serving institutions and community colleges, and from industry with knowledge and expertise in cybersecurity.

(d) REPORT.—Not later than 12 months after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall transmit to the Congress a report describing the findings and recommendations of the task force.

(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.

SEC. 109. CYBERSECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.

Section 8(c) of the Cyber Security Research and Development Act (15 U.S.C. 7406(c)) is amended to read as follows:

"(c) SECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.—

"(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government in order to enable standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security within the Federal Government.

"(2) PRIORITIES FOR DEVELOPMENT.—The Director of the National Institute of Standards and Technology shall establish priorities for the development of standards, reference materials, and checklists under this subsection on the basis of—

"(A) the security risks associated with the use of the system;

"(B) the number of agencies that use a particular system or security tool;

"(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

"(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

"(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

"(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a standard, reference material, or checklist for the system.

"(4) DISSEMINATION OF STANDARDS AND RELATED MATERIALS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

"(5) AGENCY USE REQUIREMENTS.—The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

"(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or checklist for the system;

"(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

"(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

"(D) preclude any Federal agency from procuring or deploying other information technology hardware or software systems for which no such standard, reference material, or checklist has been developed or identified under paragraph (1).".

SEC. 110. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY RESEARCH AND DEVELOPMENT.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by redesignating subsection (e) as subsection (f), and by inserting after subsection (d) the following:

"(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall—

"(1) conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies and that is amenable to implementation within a wide variety of existing and emerging computing environments;

"(2) carry out research associated with improving the security of information systems and networks;

"(3) carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks; and

"(4) carry out research associated with improving security of industrial control systems.".

TITLE II—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

SEC. 201. DEFINITIONS.

In this title:

(1) DIRECTOR.—The term "Director" means the Director of the National Institute of Standards and Technology.

(2) INSTITUTE.—The term "Institute" means the National Institute of Standards and Technology.

SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to the Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities specified in subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 203. CLOUD COMPUTING STRATEGY.

(a) IN GENERAL.—The Director, in collaboration with the Federal CIO Council, and in consultation with other relevant Federal agencies and stakeholders from the private sector, shall continue to develop and implement a comprehensive strategy for the use and broad adoption of cloud computing services by the Federal Government.

(b) ACTIVITIES.—In carrying out the strategy developed under subsection (a), the Director shall give consideration to activities that—

(1) accelerate the development of standards that address interoperability and portability of cloud computing services;

(2) support the development of conformance test systems; and

(3) address appropriate security frameworks and reference materials for use by Federal agencies to address their security and privacy requirements, including—

(A) the physical security of cloud computing data centers and the data stored in such centers; and

(B) accessibility of the data stored in cloud computing data centers.

SEC. 204. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION.

(a) PROGRAM.—The Director, in collaboration with relevant Federal agencies, industry, educational institutions, National Laboratories, and other organizations, shall continue to coordinate a cybersecurity awareness and education program to increase knowledge, skills, and awareness of cybersecurity risks, consequences, and best practices through—

(1) the widespread dissemination of cybersecurity technical standards and best practices identified by the Institute; and

(2) efforts to make cybersecurity technical standards and best practices usable by individuals, small to medium-sized businesses, State, local, and tribal governments, and educational institutions.

(b) STRATEGIC PLAN.—The Director shall, in cooperation with relevant Federal agencies and other stakeholders, develop and implement a strategic plan to guide Federal programs and activities in support of a comprehensive cybersecurity awareness and education program as described under subsection (a).

(c) REPORT TO CONGRESS.—Not later than 1 year after the date of enactment of this Act and every 5 years thereafter, the Director shall transmit the strategic plan required under subsection (b) to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

SEC. 205. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns, to—

(1) improve interoperability among identity management technologies;

(2) strengthen authentication methods of identity management systems;

(3) improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) improve the usability of identity management systems.

SEC. 206. AUTHORIZATIONS.

No additional funds are authorized to carry out this title and the amendments made by this title or to carry out the amendments made by sections 109 and 110 of this Act. This title and the amendments made by this title and the amendments made by sections 109 and 110 of this Act shall be carried out using amounts otherwise authorized or appropriated.

II. PURPOSE AND SUMMARY

The purpose of H.R. 2096 is to improve cybersecurity in the Federal, private, and public sectors through: coordination and prioritization of federal cybersecurity research and development activities; strengthening of the cybersecurity workforce; coordination of Federal agency engagement in international cybersecurity technical standards development; and the reauthorization of cybersecurity related programs at the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST).

III. BACKGROUND AND NEED FOR THE LEGISLATION

Information technology (IT) has evolved rapidly over the last decade, leading to markedly increased connectivity and productivity. The benefits provided by these advancements have led to the widespread use and incorporation of information technologies across major sectors of the economy. This level of connectivity and the dependence of our critical infrastructures on IT have also increased the vulnerability of these systems. Reports of cyber criminals and possibly nation-states accessing sensitive information and disrupting services have risen steadily over the last decade, heightening concerns over the adequacy of our cybersecurity measures.

According to the Office of Management and Budget, Federal agencies spent $8.6 billion in FY 2010 on cybersecurity, and the Federal government has spent more than $600 billion on information technology in the last decade. In addition, the Federal government funds nearly $400 million in cybersecurity research and development each year.

In January 2008, the Bush Administration established, through a series of classified executive directives, the Comprehensive National Cybersecurity Initiative (CNCI). The Obama Administration has continued this initiative, with the goal of securing Federal systems and fostering public-private cooperation. In February 2009, the Obama Administration called for a 60-day review of the national cybersecurity strategy. The President's review required the development of a framework that would ensure that the CNCI was adequately funded, integrated, and coordinated among Federal agencies, the private sector, and state and local authorities.

On May 29, 2009, the Obama Administration released its Cyberspace Policy Review. The Review recommended an increased level of interagency cooperation among all departments and agencies, highlighted the need for information sharing concerning attacks and vulnerabilities, and highlighted the need for an exchange of research and security strategies essential to the efficient and effective defense of Federal computer systems. Furthermore, it stressed the importance of advancing cybersecurity research and development, and the need for the Federal Government to partner with the private sector to guarantee a secure and reliable infrastructure. The Review also called for increased public awareness, improved education and expansion of the number of information technology professionals.

In June 2009, GAO found that the Federal agencies responsible for protecting the U.S. Information Technology (IT) infrastructure were not satisfying their responsibilities, leaving the Nation's IT infrastructure vulnerable to attack. In an effort to strengthen the work of those Federal agencies, the U.S. House of Representatives passed the Cybersecurity Enhancement Act of 2010 (H.R. 4061) in the 111th Congress by a vote of 422–5. H.R. 4061 required increased coordination and prioritization of Federal cybersecurity research and development activities, and the development and advancement of cybersecurity technical standards. It also strengthened cybersecurity education and talent development and industry partnership initiatives. The Senate did not act on the legislation.

The task of coordinating unclassified cybersecurity research and development (R&D) lies with the Networking and Information Technology Research and Development (NITRD) program, which was originally authorized in statute by the High-Performance Computing Act of 1991 (P.L. 102–194). The NITRD program, which consists of 15 Federal agencies, coordinates a broad spectrum of R&D activities related to information technology. It also includes an interagency working group and program component area focused specifically on cybersecurity and information R&D. However, many expert panels, including the President's Council of Advisors on Science and Technology, have argued that the portfolio of Federal investments in cybersecurity R&D is not properly balanced and is focused on short-term reactive technologies at the expense of long-term, fundamental R&D.

With a budget of $127 million for FY 2010, NSF is the principal agency supporting unclassified cybersecurity R&D and education. NSF's cybersecurity research activities are primarily funded through the Directorate for Computer & Information Science & Engineering (CISE). CISE supports cybersecurity R&D through a targeted program, Trustworthy Computing, as well as through a number of its core activities in Computer Systems Research, Computing Research Infrastructure, and Network and Science Engineering. In addition to its basic research activities, NSF's Directorate for Education & Human Resources (EHR) manages the Scholarship for Service program which provides funding to colleges and universities for the award of 2-year scholarships in information assurance and computer security fields.

NIST is tasked with protecting the federal information technology network by developing and promulgating cybersecurity standards for federal non-classified network systems (Federal Information Processing Standards [FIPS]), identifying methods for assessing effectiveness of security requirements, conducting tests to validate security in information systems, and conducting outreach exercises. Experts have stated that NIST's technical standards and best practices are too highly technical for general public use, and making this information more usable to average computer users with less technical expertise will help raise the base level of cybersecurity knowledge among individuals, business, education, and government.

Currently, the United States is represented on international bodies dealing with cybersecurity by an array of organizations, including the Department of State, Department of Commerce, Federal Communications Commission, and the United States Trade Representative without a coordinated and comprehensive strategy or plan. The Cyberspace Policy Review called for a comprehensive international cybersecurity strategy that defines what cybersecurity standards we need, where they are being developed, and ensures that the United States Federal government has agency representation for each. Recognizing that private sector standards development organizations also are engaged in international standards work, in some scenarios a nonfederal entity may be best equipped to represent United States interests, and coordination is necessary.

In the 107th Congress, the Science and Technology Committee developed the Cyber Security Research and Development Act (P.L. 107–305). The bill created new programs and expanded existing programs at NSF and NIST for computer and network security. The authorizations established under the Cyber Security Research and Development Act expired in fiscal year 2007.

IV. Hearing Summary

In the 111th Congress, the House Committee on Science and Technology held four subcommittee hearings to explore the state of Federal cybersecurity research and development, education, and workforce training programs; to review the findings and recommendations included in the Administration's Cyberspace Policy Review; to examine ways Federal cybersecurity efforts could enhance privately-owned critical infrastructure, better monitor Federal networks, and more clearly define performance metrics and

success criteria; and to review the findings and recommendations of a report from the Government Accountability Office (GAO)[1]. Both the review and the report called for an increase in effective public/private partnerships, and for clarification of agency roles and responsibilities. As a result of information gathered from the hearings, H.R. 4061, the Cybersecurity Enhancement Act, was introduced on a bipartisan basis on November 7, 2009. The Science and Technology Committee favorably reported the bill on January 27, 2010, and the House passed the measure on February 4, 2010 by a vote of 422–5. The Senate did not act on this measure prior to the adjournment of the 111th Congress.

In the 112th Congress, the Subcommittee on Technology and Innovation and the Subcommittee on Research and Science Education held a joint hearing on May 25, 2011, to examine Federal agency efforts to improve our national cybersecurity and prepare the future cybersecurity talent needed for national security. The hearing included updates from the agencies on how they are responding to and addressing objectives of the 2009 Cyberspace Policy Review, their efforts to educate and develop the necessary cybersecurity personnel, and how standards development is coordinated with other relevant agencies.

The Subcommittees heard from four Federal government witnesses: Dr. George O. Strawn, Director of the National Coordination Office for the Networking and Information Technology Research and Development Program; Dr. Farnam Jahanian, Assistant Director of the Directorate for Computer and Information Science and Engineering at the National Science Foundation; Ms. Cita Furlani, Director of the Information Technology Laboratory at the National Institute of Standards and Technology; and Rear Admiral Michael Brown, Director of Cybersecurity Coordination in the National Protection and Programs Directorate for the U.S. Department of Homeland Security

V. Committee Consideration

On June 2, 2011, Representative Mike McCaul (R–TX), for himself, and Representative Daniel Lipinski (D–IL), introduced H.R. 2096, the Cybersecurity Enhancement Act of 2011, a bill to advance cybersecurity research, development, and technical standards, and for other purposes. H.R. 2096 was referred to the Committee on Science, Space, and Technology.

On July 21, 2011, the Committee on Science, Space, and Technology met in open markup session and ordered H.R. 2096 favorably reported to the House, as amended, by voice vote.

VI. Committee Votes

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. A motion to order H.R. 2096 favorably reported to the House, as amended, was agreed to by voice vote.

During Full Committee consideration of H.R. 2096, the following amendments were considered:

---

[1] National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture, Government Accountability Office, http://www.gao.gov/new.items/d09432t.pdf

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Full Committee Markup
July 21, 2011

AMENDMENT ROSTER

H. R. 2096, the "Cybersecurity Enhancement Act of 2011"

No.	Amendment	Summary	Results
1	Mr. McCaul/Lipinski (024)	Makes minor clarifications to the Cybersecurity University-Industry Task Force section and technical changes to the bill; updates several provisions specific to the NIST activities in cybersecurity; includes language clarifying that no additional funds are authorized for NIST activities in the bill.	Agreed to by Voice Vote
2	Amendment Offered by Mr. McNerney (025) To McCaul Amendment (024)	Adds "National Laboratories" to the list of stakeholders with which the Director of NIST shall continue to coordinate a cybersecurity education and awareness program (sec. 203).	Agreed to by Voice Vote
3	REVISED Amendment Offered by Ms. Johnson (040) To McCaul Amendment (024)	Amends manager's amendment to expand the responsibilities of NIST's education and awareness program beyond their technical standards and best practices expertise to include a focus on improving formal cybersecurity programs and activities at all education levels, Federal workforce preparation, and public awareness, among other things.	Withdrawn
4	Mr. Lujan (030)	Amends the strategic plan in Section 103 to ensure it describes how the program will include technologies to protect consumer privacy.	En Bloc Amendment (1 of 6) Agreed to by Unanimous Consent
5	Mr. Lujan (032)	Amends the strategic plan to ensure that it is focused on how the program can ensure the "rapid" transfer of results from cybersecurity research and development and a "timely" benefit to society.	En Bloc Amendment (2 of 6) Agreed to by Unanimous Consent

6	Mr. Lujan (033)	Adds "National Laboratories" to the list of stakeholders that the agencies should solicit advice and recommendations from in the development of the strategic plan.	En Bloc Amendment (3 of 6) Agreed to by Unanimous Consent
7	Mr. Smith (042)	Adds language to the workforce assessment section to require review of the ability of universities to provide training and education in critical skills on cybersecurity; changes the focus of the cybersecurity task force to require the task force to explore mechanisms for "education and training" on cybersecurity as well as research and development.	En Bloc Amendment (4 of 6) Agreed to by Unanimous Consent
8	Ms. Fudge (027)	Requires the workforce assessment as it reviews the effectiveness of certain government programs in producing cybersecurity professionals to include areas with high unemployment .	En Bloc Amendment (5 of 6) Agreed to by Unanimous Consent
9	Mr. Clarke (CYBER11_003)	Strikes a research provision currently included in section 110 and inserts it into section 204; further builds upon existing provisions of section 204 to include the development of an implementation plan for the Federal government to provide and use identity management technologies.	Not Agreed to by Voice Vote
10	Mr. Lipinski (032)	Directs NIST to continue to develop and implement a comprehensive strategy for the use and adoption of cloud computing services by the Federal government.	En Bloc Amendment (6 of 6) Agreed to by Unanimous Consent
11	Mr. Wu (020)	Adds a new section providing NIST the authority to convene stakeholders within the information services sectors (e.g. content, storage, internet transactions) in order to develop consensus standards and voluntary codes of conduct for information security.	Withdrawn
12	Mr. Wu (019)	Requires NIST as part of the cybersecurity education and awareness program in section 203 to carry out an assessment of community colleges role in cybersecurity education and the development of a skilled cybersecurity workforce.	Withdrawn

13	Mr. Tonko (CYBER11_001)	The Director of the Office of Science and Technology Policy (OSTP) is not required to carry out the activities of the Cybersecurity University-Industry Task Force (sec. 108) unless the appropriation for OSTP for any fiscal year is equal or higher to FY11 appropriations. The same limitation is also included for the Director of NIST to carry out certain cybersecurity activities in research and development (sec. 110), international cybersecurity standards (sec. 202), and education and awareness (sec. 203).	Not Agreed to by a roll call vote of 13 Yeas and 17 Noes

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 AMENDMENT NO. 001 ROLL CALL NO. 1

Bill: H. R. 2096
SPONSOR: Mr. Tonko

Not agreed to by a vote of 13 yeas and 17 nays

Quorum –14 to vote –21 to report

MEMBER	AYE	NO	PRESENT	NOT VOTING
1 Mr. HALL, ***Chair*** - TX		X		
2 Mr. SENSENBRENNER – WI **		X		
3 Mr. SMITH - TX		X		
4 Mr. ROHRABACHER - CA		X		
5 Mr. BARTLETT - MD		X		
6 Mr. LUCAS - OK				
7 Mrs. BIGGERT - IL		X		
8 Mr. AKIN - MO				
9 Mr. NEUGEBAUER - TX				
10 Mr. McCAUL - TX		X		
11 Mr. BROUN - GA		X		
12 Mrs. ADAMS - FL		X		
13 Mr. QUAYLE - AZ				
14 Mr. FLEISCHMANN - TN		X		
15 Mr. RIGELL - VA		X		
16 Mr. PALAZZO - MS		X		
17 Mr. BROOKS - AL		X		
18 Mr. HARRIS - MD		X		
19 Mr. HULTGREN - IL		X		
20 Mr. CRAVAACK - MN		X		
21 Mr. BUCSHON - IN				
22 Mr. BENISHEK - MI		X		
23 Vacancy				
1 Ms. JOHNSON, ***Ranking*** - TX	X			
2 Mr. COSTELLO - IL	X			
3 Ms. WOOLSEY - CA				
4 Ms. LOFGREN - CA	X			
5 Mr. WU - OR	X			
6 Mr. MILLER - NC				
7 Mr. LIPINSKI - IL	X			
8 Ms. GIFFORDS - AZ				
9 Ms. EDWARDS - MD	X			
10 Ms. FUDGE - OH	X			
11 Mr. LUJÁN - NM	X			
12 Mr. TONKO - NY	X			
13 Mr. McNERNEY - CA	X			
14 Mr. SARBANES - MD				
15 Ms. SEWELL - AL	X			
16 Ms. WILSON - FL	X			
17 Mr. CLARKE - MI	X			
TOTALS	13	17		

** Vice Chair

VII. Summary of Major Provisions of the Bill

The bill requires that the agencies participating in the National Information Technology Research and Development (NITRD) program develop a strategic plan to guide the overall direction of Federal cybersecurity and information assurance R&D. It requires the agencies to solicit recommendations and advice from the advisory committee and a wide range of stakeholders and that they develop an implementation roadmap for the strategic plan.

The bill reauthorizes cybersecurity workforce and traineeship programs at NSF, including through the Advanced Technological Education program, the Integrative Graduate Education and Research traineeship program and the Graduate Research Fellowship program. It also requires the President to conduct an assessment of cybersecurity workforce needs across the Federal government and formally codifies NSF to carry out the Scholarship for Service program.

Additionally, the bill reauthorizes cybersecurity research at NSF, including through the Trustworthy Computing program and it requires that the Director of the Office of Science and Technology Policy convene a university-industry task force to explore mechanisms for carrying out collaborative R&D.

The bill amends section 8(c) of the Cybersecurity R&D Act (15 U.S.C. 7406(c)) by requiring the Director of NIST to develop and revise as necessary, security automation standards, checklists, configuration profiles, and deployment recommendations for products and protocols that minimize the security risks associated with each information technology hardware or software system used by the Federal government. The bill also amends section 20 of the NIST Act (15 U.S.C. 278g–3), by directing NIST to conduct a research program aimed at creating a standardized identity, privilege, and access control management framework that can be used to enforce a wide variety of resource protection policies. The framework should be usable in a wide variety of existing and emerging computing environments. The bill also directs NIST to conduct research on how to improve the security of information systems, networks, and industrial control systems.

The bill directs NIST to coordinate with other Federal agencies and private sector stakeholders involved in international cybersecurity technical standards development and to report to Congress on a plan to conduct this coordination within one year of enactment.

NIST is also required to deliver a plan to Congress, within one year of enactment, describing how it will continue to coordinate a cybersecurity awareness and education program. NIST is to collaborate with relevant Federal agencies, National Laboratories, industry and educational institutions in developing this program. The purpose of the program is to disseminate cybersecurity best practices and standards and to make these standards and practices usable by individuals, small to medium-sized businesses, state and local governments and educational institutions. NIST is also directed to develop a strategic plan to implement the program.

The bill directs NIST to engage in research and development programs to improve identity management systems. The programs have the goals of improving interoperability among identity man-

agement technologies, strengthening authentication methods, and improving privacy protection.

The bill clarifies that no additional funds are authorized for the NIST programs in the bill.

VIII. COMMITTEE VIEWS

Cybersecurity strategic R&D Plan and implementation roadmap

The Committee expects the strategic plan to be a useful guide for setting program priorities and estimating time scales for reaching program objectives. The strategic plan should not be limited to time scales of 2 to 3 years, but should include mid-term and long-term research objectives based on known research gaps and an assessment of cybersecurity risks to ensure that R&D objectives are informed and prioritized by the Nation's needs. Furthermore, the Committee intends for the development of the plan to be informed by the research needs of industry and academia and expects the National Coordination Office to actively solicit stakeholder input through meetings, requests for information and other appropriate means.

The Committee believes the development of an implementation roadmap is essential to the furtherance of cybersecurity and information assurance R&D. The roadmap should be aligned with the program's strategic plan and overall objectives, and should be detailed enough to clearly define the roles and responsibilities of individual Federal agencies in the achievement of the overall R&D objectives. While each Federal agency has its own mission and objectives in the area of cybersecurity and information assurance, the Committee considers the development of an implementation roadmap essential to comprehensively addressing our cybersecurity challenges.

Cybersecurity education and workforce

Over the next several years, the Bureau of Labor Statistics estimates that the number of jobs requiring a background in computer science or mathematics will average approximately 150,000 annually. However, the number of computer science undergraduate degrees granted has dropped 26 percent from 2003 to 2007. Additionally, according to the report entitled, "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce," there is a shortfall of between 500 and 1,000 cybersecurity professionals each year across the Federal government. The Committee believes that the required assessment of Federal cybersecurity workforce needs, necessary skills, and the capacity of our colleges and universities, including community colleges, to produce cybersecurity professionals is an essential first step in ensuring an adequate, well-trained workforce.

As part of the Workforce Training Assessment, the Committee expects that any assessment of education and training activities also include activities considered to be outside the scope of a classroom such as simulations and competitions. When promoting cybersecurity awareness and education for the public, NIST should fully utilize existing resources within the Federal government, private industry, academia, and independent organizations to minimize duplicative effort.

Cybersecurity University—Industry task force

In considering options for a collaborative model for carrying out cybersecurity research and development, it is the Committee's intention that the objective of such a potential entity would be to supplement, not supplant, the traditional functions and activities of the individual participating entities. Therefore, in developing guidelines in accordance with subsection (b)(2) of this section, it is the Committee's expectation that the task force work to identify activities that (1) would address nationally significant challenges that advance common objectives; and (2) require collaboration that could not otherwise be reasonably addressed by individual entities acting independently.

NIST's security automation and checklist development and dissemination

The Committee believes that advancements of technology have presented an opportunity to evolve security checklists into automated auditing programs capable of verifying information security policy compliance, as well as the measurement and management of vulnerabilities. NIST's Security Content Automation Protocol program is an excellent example of a public-private partnership developing interoperable security specifications to automate the assessment, documentation, and reporting of information security requirements. The Committee also believes that NIST should be more proactive in disseminating checklists to other Federal agencies.

International cybersecurity technical standards

The Committee intends for NIST to coordinate Federal agency engagement in international cybersecurity technical standards development, in partnership with relevant Federal agencies. This provision is meant to recognize that coordinating cybersecurity standards efforts across different Federal agencies will ensure appropriate governmental representation at international standard dialogues. Furthermore, in some instances it may not be appropriate for Federal agencies to be directly involved in the development of international cybersecurity technical standards. Therefore, consultation with private stakeholders is also required to determine the appropriate level of engagement, if any, by Federal agencies in specific international cybersecurity technical standards matters. Given the global nature of networked systems, it is imperative that the Federal government has a coordinated, comprehensive strategy to address international cybersecurity technical standards needs.

Cloud computing strategy

The Committee recognizes the economic potential of the public and private sector's utilization of cloud computing. However, stakeholders must be certain their information will be secure in the cloud. NIST, working in close conjunction with industry, is well-positioned to provide standards and protocols to ensure that the cloud is a safe system for the Federal government to utilize.

IX. Committee Oversight Findings

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held an oversight hearing and made findings that are reflected in the descriptive portions of this report.

X. Statement on General Performance Goals and Objectives

In accordance with clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the performance goals and objectives of the Committee are reflected in the descriptive portions of this report, including the goal to improve cybersecurity in the Federal, private, and public sectors and to protect the Nation's critical infrastructure.

XI. New Budget Authority, Entitlement Authority, and Tax Expenditures

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

XII. Advisory on Earmarks

In compliance with clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 2096, the Cybersecurity Enhancement Act of 2011, contains no earmarks.

XIII. Committee Cost Estimate

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

XIV. Congressional Budget Office Cost Estimate

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

August 24, 2011.

Hon. Ralph M. Hall,
Chairman, Committee on Science, Space, and Technology,
House of Representatives, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2096, the Cybersecurity Enhancement Act of 2011.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Martin von Gnechten.

Sincerely,

Douglas W. Elmendorf.

Enclosure.

H.R. 2096—Cybersecurity Enhancement Act of 2011

Summary: H.R. 2096 would reauthorize several National Science Foundation (NSF) programs that aim to enhance cybersecurity (the protection of computers and computer networks from unauthorized access). The bill also would require the National Institute of Standards and Technology (NIST) to continue a cybersecurity awareness program and to develop standards for managing personal identifying information stored on computer systems. Finally, the bill would establish a task force to recommend actions to the Congress for improving cybersecurity research and development.

Based on information from NSF and NIST and assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 2096 would cost $382 million over the 2012–2016 period and $39 million after 2016. Enacting the legislation would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

H.R. 2096 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 2096 is shown in the following table. The costs of this legislation fall within budget function 250 (general science, space, and technology).

	By fiscal year, in millions of dollars—					
	2012	2013	2014	2015	2016	2012–2016
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
NSF Cybersecurity Research Grants:						
Authorization Level	90	90	90	0	0	270
Estimated Outlays	12	48	71	73	41	245
NSF Cybersecurity Research Centers:						
Authorization Level	5	5	5	0	0	14
Estimated Outlays	1	2	4	4	2	12
NSF Cybersecurity Capacity Building Grants:						
Authorization Level	19	19	19	0	0	57
Estimated Outlays:	2	10	15	15	9	52
NSF Science and Advanced Technology Grants:						
Authorization Level	3	3	3	0	0	8
Estimated Outlays	*	1	2	2	1	7
NSF Cybersecurity Graduate Traineeships:						
Authorization Level	24	24	24	0	0	72
Estimated Outlays	3	13	19	19	11	65
Cybersecurity Task Force:						
Estimated Authorization Level	1	0	0	0	0	1
Estimated Outlays	1	0	0	0	0	1
Total Changes under H.R. 2096:						
Estimated Authorization Level	141	140	140	0	0	421
Estimated Outlays	19	74	111	113	64	382

Notes: NSF = National Science Foundation; * = less than $500,000.
Amounts may not sum to totals because of rounding.

Basis of estimate: For this estimate, CBO assumes that H.R. 2096 will be enacted near the end of 2011 and that the authorized and necessary amounts will be appropriated each fiscal year. Estimated outlays are based on historical spending patterns for NSF and NIST programs.

H.R. 2096 would authorize appropriations for several NSF grant programs aimed at enhancing cybersecurity. The bill would authorize appropriations totaling $270 million over the 2012–2014 period

to improve research on cybersecurity. H.R. 2096 would authorize $14 million in grants to establish centers of cybersecurity research. The bill also would authorize $57 million in grants for universities to improve cybersecurity programs and increase the number students in the fields related to cybersecurity. This includes a program to offer scholarships to students who pursue higher education related to cybersecurity and commit to public service after graduating. H.R. 2096 would authorize the appropriation of $72 million for grants to higher education institutions to establish cybersecurity traineeship programs for graduate students. The bill also would authorize $8 million in grants for associate-degree-granting institutions to develop cybersecurity programs and establish centers of excellence.

H.R. 2096 would establish a task force of academic and industry experts to advise the Office of Science and Technology Policy on issues related to cybersecurity. Based on information regarding the cost of funding similar activities, CBO estimates that carrying out this provision would cost $1 million over the 2012–2016 period.

H.R. 2096 also would direct NIST to establish standards and protocols to enhance cybersecurity, to develop a strategy for the government to adopt cloud computing services (the use of servers and network storage to provide remote, on-demand access to shared computer applications and services), and to promote cybersecurity awareness and education. Based on information from NIST, CBO estimates that these activities would have no significant impact on the federal budget.

Pay-As-You-Go consideration: None.

Intergovernmental and private-sector impact: H.R. 2096 contains no intergovernmental or private-sector mandates as defined in UMRA and would impose no costs on state, local, or tribal governments.

Estimate prepared by: Federal costs: Martin von Gnechten; Impact on state, local, and tribal governments: Elizabeth Cove Delisle; Impact on the private sector: Sam Wice and Patrice Gordon.

Estimate approved by: Peter H. Fontaine, Assistant Director for Budget Analysis.

XV. Federal Mandates Statement

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

XVI. Federal Advisory Committee Statement

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

XVII. Applicability to Legislative Branch

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

XVIII. SECTION-BY-SECTION ANALYSIS

TITLE I—RESEARCH AND DEVELOPMENT

Sec. 101. Definitions

Defines the terms National Coordination Office and Program in the title.

Sec. 102. Findings

Describes the findings of this title.

Sec. 103. Cybersecurity strategic R&D plan

Requires the agencies to develop, update and implement a strategic plan for cybersecurity research and development (R&D). Requires that the strategic plan be based on an assessment of cybersecurity risk, that it specify and prioritize near-term, mid-term and long-term research objectives, and that it describe how the near-term objectives complement R&D occurring in the private sector. Requires the agencies to solicit input from an advisory committee and outside stakeholders in the development of the strategic plan. Additionally, it requires the agencies to describe how they will promote innovation, foster technology transfer, and maintain a national infrastructure for the development of secure, reliable, and resilient networking and information technology systems.

Requires the development of an implementation roadmap that specifies the role of each agency and the level of funding needed to meet each of the research objectives outlined in the strategic plan.

Sec. 104. Social and behavioral research in cybersecurity

Requires the National Science Foundation (NSF) to support research on the social and behavioral aspects of cybersecurity as part of its total cybersecurity research portfolio.

Sec. 105. NSF Cybersecurity R&D programs

Reauthorizes the cybersecurity research program at the NSF and includes identity management as one of the research areas supported.

Reauthorizes programs at NSF that provide funding for capacity building grants, graduate student fellowships, graduate student traineeships and research centers in cybersecurity.

Sec. 106. Federal cyber scholarship for service program

Authorizes the cybersecurity scholarship for service program at NSF as part of cybersecurity capacity grants. The program provides grants to institutions of higher education for the award of scholarships to students pursuing undergraduate and graduate degrees in cybersecurity fields. It further requires service as a cybersecurity professional in the Federal government as a condition of the scholarship to equal one year more than the length of the scholarship.

Sec. 107. Cybersecurity workforce assessment

Requires the President to issue a report assessing the current and future cybersecurity workforce needs of the Federal government, including a comparison of the skills sought by Federal agen-

cies and the private sector; an examination of the supply of cybersecurity talent and the capacity of institutions of higher education to produce cybersecurity professionals; and the identification of any barriers to the recruitment and hiring of cybersecurity professionals.

Sec. 108. Cybersecurity university-industry task force

Establishes a university-industry task force to explore mechanisms and models for carrying out public-private research partnerships in the area of cybersecurity.

Sec. 109. Cybersecurity checklist and dissemination

Updates NIST's authority for the National Checklist Program (NCP), which provides detailed guidance on setting the security configuration of operating systems and applications and requires NIST to develop automated security specifications with respect to checklist content. The section updates language originally provided in the Cyber Security Research and Development Act of 2002, ensuring that the technical wording reflects the current state of the art, which has advanced to include more automated procedures.

Sec. 110. NIST cybersecurity R&D

Amends the National Institute of Standards and Technology Act to authorize NIST, as part of its in-house research program, to continue efforts to develop a unifying and standardized identity, privilege, and access control management framework. Authorizes NIST to conduct research related to improving the security of information and networked systems, including the security of industrial control systems.

TITLE II—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

Sec. 201. Definitions

Defines the terms Director and Institute in the title.

Sec. 202. International cybersecurity technical standards

Directs NIST to develop and implement a plan to ensure coordination between Federal agencies on international cybersecurity technical standards development. This plan is due to Congress no later than one year after enactment. The provision clarifies that government representation is not mandatory and ensures coordination with non-governmental stakeholders.

Sec. 203. Cloud computing strategy

Directs NIST, in collaboration with Federal agencies and other stakeholders, to continue to develop and implement a comprehensive strategy for the use and adoption of cloud computing services by the Federal government. The strategy should consider activities that accelerate standards development, the development of processes to test standards conformance, and the security of data stored in the cloud.

Sec. 204. Promoting cybersecurity awareness and education

Directs NIST to deliver a plan to Congress within one year describing how it will continue to coordinate a cybersecurity aware-

ness and education program. The program shall be aimed at disseminating cybersecurity best practices and standards and shall include how NIST will make these usable by individuals, small business, state and local governments, and educational institutions.

Sec. 205. Identity management research and development

NIST shall engage in research and development programs to improve identity management systems.

Sec. 206.

States that no additional funds are authorized for the NIST activities in the bill.

XIX. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

* * * * * * *

SEC. 2. FINDINGS.

The Congress finds the following:

[(1) Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational infrastructures—including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services—in a vast, interdependent physical and electronic network.]

(1) Advancements in information and communications technology have resulted in a globally interconnected network of government, commercial, scientific, and education infrastructures, including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services.

(2) [Exponential increases in interconnectivity have facilitated enhanced communications, economic growth,] *These advancements have significantly contributed to the growth of the United States economy* and the delivery of services critical to the public welfare, but have also increased the consequences of temporary or prolonged failure.

[(3) A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results "clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure".]

(3) The Cyberspace Policy Review published by the President in May, 2009, concluded that our information technology and communications infrastructure is vulnerable and has "suffered intrusions that have allowed criminals to steal hundreds of mil-

lions of dollars and nation-states and other entities to steal intellectual property and sensitive military information".

* * * * * * *

[(6) While African-Americans, Hispanics, and Native Americans constitute 25 percent of the total United States workforce and 30 percent of the college-age population, members of these minorities comprise less than 7 percent of the United States computer and information science workforce.**]**

(6) While African-Americans, Hispanics, and Native Americans constitute 33 percent of the college-age population, members of these minorities comprise less than 20 percent of bachelor degree recipients in the field of computer sciences.

* * * * * * *

SEC. 4. NATIONAL SCIENCE FOUNDATION RESEARCH.

(a) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—

(1) IN GENERAL.—The Director shall award grants for basic research on innovative approaches to the structure *and usability* of computer and network hardware and software that are aimed at enhancing computer security. Research areas may include—

(A) authentication, cryptography, *identity management,* and other secure data communications technology;

* * * * * * *

(H) remote access and wireless security; **[**and**]**

(I) enhancement of law enforcement ability to detect, investigate, and prosecute cyber-crimes, including those that involve piracy of intellectual property*, crimes against children, and organized crime; and***[**.**]**

(J) social and behavioral factors, including human-computer interactions, usability, and user motivations.

* * * * * * *

(3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

[(A) $35,000,000 for fiscal year 2003;
[(B) $40,000,000 for fiscal year 2004;
[(C) $46,000,000 for fiscal year 2005;
[(D) $52,000,000 for fiscal year 2006; and
[(E) $60,000,000 for fiscal year 2007.**]**
(A) $90,000,000 for fiscal year 2012;
(B) $90,000,000 for fiscal year 2013; and
(C) $90,000,000 for fiscal year 2014.

(b) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—

(1) * * *

* * * * * * *

(4) APPLICATIONS.—An institution of higher education, nonprofit research institution, or consortia thereof seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) * * *

* * * * * * *

(C) how the Center will contribute to increasing the number and quality of computer and network security researchers and other professionals, including individuals from groups historically underrepresented in these fields; [and]

(D) how the center will disseminate research results quickly and widely to improve cyber security in information technology networks, products, and services[.]*; and*

(E) how the center will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions.

* * * * * * *

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the National Science Foundation to carry out this subsection—

[(A) $12,000,000 for fiscal year 2003;
[(B) $24,000,000 for fiscal year 2004;
[(C) $36,000,000 for fiscal year 2005;
[(D) $36,000,000 for fiscal year 2006; and
[(E) $36,000,000 for fiscal year 2007.]
(A) $4,500,000 for fiscal year 2012;
(B) $4,500,000 for fiscal year 2013; and
(C) $4,500,000 for fiscal year 2014.

SEC. 5. NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—

(1) * * *

* * * * * * *

(6) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

[(A) $15,000,000 for fiscal year 2003;
[(B) $20,000,000 for fiscal year 2004;
[(C) $20,000,000 for fiscal year 2005;
[(D) $20,000,000 for fiscal year 2006; and
[(E) $20,000,000 for fiscal year 2007.]
(A) $19,000,000 for fiscal year 2012;
(B) $19,000,000 for fiscal year 2013; and
(C) $19,000,000 for fiscal year 2014.

(b) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT OF 1992.—

(1) * * *

(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

[(A) $1,000,000 for fiscal year 2003;
[(B) $1,250,000 for fiscal year 2004;
[(C) $1,250,000 for fiscal year 2005;
[(D) $1,250,000 for fiscal year 2006; and
[(E) $1,250,000 for fiscal year 2007.]
(A) $2,500,000 for fiscal year 2012;

(B) $2,500,000 for fiscal year 2013; and
(C) $2,500,000 for fiscal year 2014.

(c) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—

(1) * * *

* * * * * * *

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

[(A) $10,000,000 for fiscal year 2003;
[(B) $20,000,000 for fiscal year 2004;
[(C) $20,000,000 for fiscal year 2005;
[(D) $20,000,000 for fiscal year 2006; and
[(E) $20,000,000 for fiscal year 2007.]
(A) $24,000,000 for fiscal year 2012;
(B) $24,000,000 for fiscal year 2013; and
(C) $24,000,000 for fiscal year 2014.

* * * * * * *

[(e) CYBER SECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—

[(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs to enable graduate students to pursue academic careers in cyber security upon completion of doctoral degrees.

[(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

[(3) APPLICATION.—Each institution of higher education desiring to receive a grant under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director shall require.

[(4) USE OF FUNDS.—Funds received by an institution of higher education under this paragraph shall—

[(A) be made available to individuals on a merit-reviewed competitive basis and in accordance with the requirements established in paragraph (7);

[(B) be in an amount that is sufficient to cover annual tuition and fees for doctoral study at an institution of higher education for the duration of the graduate traineeship, and shall include, in addition, an annual living stipend of $25,000; and

[(C) be provided to individuals for a duration of no more than 5 years, the specific duration of each graduate traineeship to be determined by the institution of higher education, on a case-by-case basis.

[(5) REPAYMENT.—Each graduate traineeship shall—

[(A) subject to paragraph (5)(B), be subject to full repayment upon completion of the doctoral degree according to a repayment schedule established and administered by the institution of higher education;

[(B) be forgiven at the rate of 20 percent of the total amount of the graduate traineeship assistance received under this section for each academic year that a recipient

is employed as a full-time faculty member at an institution of higher education for a period not to exceed 5 years; and

[(C) be monitored by the institution of higher education receiving a grant under this subsection to ensure compliance with this subsection.

[(6) EXCEPTIONS.—The Director may provide for the partial or total waiver or suspension of any service obligation or payment by an individual under this section whenever compliance by the individual is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

[(7) ELIGIBILITY.—To be eligible to receive a graduate traineeship under this section, an individual shall—

[(A) be a citizen, national, or lawfully admitted permanent resident alien of the United States; and

[(B) demonstrate a commitment to a career in higher education.

[(8) CONSIDERATION.—In making selections for graduate traineeships under this paragraph, an institution receiving a grant under this subsection shall consider, to the extent possible, a diverse pool of applicants whose interests are of an interdisciplinary nature, encompassing the social scientific as well as the technical dimensions of cyber security.

[(9) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this paragraph $5,000,000 for each of fiscal years 2003 through 2007.]

* * * * * * *

SEC. 8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY PROGRAMS.

(a) * * *

* * * * * * *

[(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

[(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government.

[(2) PRIORITIES FOR DEVELOPMENT; EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may establish priorities for the development of checklists under this paragraph on the basis of the security risks associated with the use of the system, the number of agencies that use a particular system, the usefulness of the checklist to Federal agencies that are users or potential users of the system, or such other factors as the Director determines to be appropriate. The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any computer hardware or software system for which the Director of the National Institute of Standards and Technology determines that the development of a checklist is inappropriate because of the infrequency of use of the system, the obsoles-

cence of the system, or the inutility or impracticability of developing a checklist for the system.

[(3) DISSEMINATION OF CHECKLISTS.—The Director of the National Institute of Standards and Technology shall make any checklist developed under this paragraph for any computer hardware or software system available to each Federal agency that is a user or potential user of the system.

[(4) AGENCY USE REQUIREMENTS.—The development of a checklist under paragraph (1) for a computer hardware or software system does not—

[(A) require any Federal agency to select the specific settings or options recommended by the checklist for the system;

[(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

[(C) represent an endorsement of any such system by the Director of the National Institute of Standards and Technology; nor

[(D) preclude any Federal agency from procuring or deploying other computer hardware or software systems for which no such checklist has been developed.]

(c) SECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.—

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government in order to enable standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security within the Federal Government.

(2) PRIORITIES FOR DEVELOPMENT.—The Director of the National Institute of Standards and Technology shall establish priorities for the development of standards, reference materials, and checklists under this subsection on the basis of—

(A) the security risks associated with the use of the system;

(B) the number of agencies that use a particular system or security tool;

(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any information technology hardware or software system or security tool for which such Director de-

termines that the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a standard, reference material, or checklist for the system.

(4) DISSEMINATION OF STANDARDS AND RELATED MATERIALS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

(5) AGENCY USE REQUIREMENTS.—The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or checklist for the system;

(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

(D) preclude any Federal agency from procuring or deploying other information technology hardware or software systems for which no such standard, reference material, or checklist has been developed or identified under paragraph (1).

* * * * * * *

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

* * * * * * *

SEC. 20. (a) * * *

* * * * * * *

(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall—

(1) conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies and that is amenable to implementation within a wide variety of existing and emerging computing environments;

(2) carry out research associated with improving the security of information systems and networks;

(3) carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks; and

(4) carry out research associated with improving security of industrial control systems.

[(e)**]** *(f)* As used in this section—

(1) * * *

* * * * * * *

XX. PROCEEDINGS OF THE FULL COMMITTEE MARKUP ON H.R. 2096, THE CYBERSECURITY ENHANCEMENT ACT OF 2011

The Committee met, pursuant to call, at 10:07 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Ralph Hall [Chairman of the Committee] presiding.

THURSDAY, JULY 21, 2011

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
WASHINGTON, D.C.

Chairman HALL. Good morning. The Committee on Science, Space, and Technology will come to order.

Pursuant to notice, the Committee on Science, Space, and Technology meets today to consider the following measure: H.R. 2096, the Cybersecurity Enhancement Act of 2011, and we will proceed with the markup. We will make opening statements.

Mr. SENSENBRENNER. Mr. Chairman, I ask unanimous consent that the Chair be authorized to roll votes today and cluster them so that Members can participate as much as they can in this Committee and the other Committees that they have conflicting obligations with.

Chairman HALL. Is there objection? The Chair hears none. Do you have a question, anybody? To roll the votes where we can get out of here on time. That way if I let people speak past five minutes, why, it is my mistake. That is not going to happen today. And we will roll the votes. You will know when the votes are taken just like we will know when the votes are taken. It is so ordered.

Now we will proceed with the markup, again on the opening statements, and I will begin. I yield myself five minutes, and we are going to be held to five minutes. Please hold me to five minutes, and tap me on the shoulder if I go past. I am beginning right now.

I am very pleased to convene the markup this morning for consideration of H.R. 2096, the Cybersecurity Enhancement Act of 2011. As our reliance on information technology expands, so do our vulnerabilities. Protecting the Nation's cyber infrastructure is a responsibility shared by different federal agencies, including the National Science Foundation and the National Institute of Standards and Technology.

I am delighted that Congressmen McCaul and Lipinski have reintroduced the Cybersecurity Enhancement Act of 2011, which primarily addresses important cybersecurity efforts conducted by NSF and NIST. This passed last year out of this Committee and didn't make it to the Senate.

This bill will help to support these efforts through reauthorization of activities in four general areas. First, strategic planning for cybersecurity R&D needs across the Federal Government. Second,

basic research at the National Science Foundation, which will hopefully increase security over the long term. Third, enhanced NSF scholarships—and by the way, we are spending about $17 million on these alone, so they are very important—to increase the size and skills of the cybersecurity workforce. And fourth, strengthened R&D, standards development and coordination, and public outreach at the National Institute of Standards and Technology related to cybersecurity.

These are modest but important changes that will help us do a better job of protecting our cyber networks, and I am pleased to join as a cosponsor, along with Mr. Smith, Mr. Brooks, Mr. Wu, and Mr. Luján.

This is a good bill, and it represents a small but important step in Congress's overall efforts to address cybersecurity issues. By strengthening agency coordination and cooperation on cybersecurity research and development efforts, the bill will help address the comprehensive cybersecurity needs of the Nation.

I want to thank Mr. McCaul and Mr. Lipinski for collaborating on this bipartisan effort, and I look forward to continued cooperative efforts as we move forward.

As longstanding Members of the Science, Space, and Technology Committee know, as we all know, the Committee enjoys a tradition of bipartisanship, and as evidenced by the legislation before us today, this spirit of cooperation lives on in the 112th Congress. I thank the gentleman from Texas and the gentleman from Illinois for setting this example.

It is in that spirit of cooperation, that I seek to address concerns expressed in regard to legislation taken up by this Committee. As you are all well aware, the Republican Leadership put forward legislative protocols for the 112th Congress. The protocols are intended to guide the Majority leadership in the scheduling and consideration of legislation on the House floor. While the protocols do not govern the introduction of legislation, good-faith compliance with the protocols will be necessary if such legislation is scheduled for the floor. In other words, the protocols do not bar introduction of legislation and provide that as Committees work through the legislative process, good-faith efforts to address and comply with the protocols can be accomplished at the Committee level.

In that vein, we have an open dialogue with leadership on this legislation, and any legislation, for that matter, as it is a priority for the Committee on both sides of the aisle. We do want to get to the floor with our efforts, with our product.

In my remarks at our organizational meeting in February, I mentioned two policies which I wanted the Committee to abide by when considering legislation. The first dealt with the goal that the Committee will no longer consider bills that authorize "such sums as may be necessary." For example, the legislation in front of us today, in the previous Congress, included at least five instances of the following authorization of appropriations language, "There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the five fiscal years 2010 through 2014." During the 110th and 111th Congress, my Republican colleagues routinely offered amendments that eliminated the phrase "such sums as are necessary." That is the phrase which we do not want this Committee to utilize.

This is balanced with the desire to continue to provide agencies with the flexibility within a defined amount of funding for the myriad of activities we may direct them to conduct. We continue to work through options by which to satisfy this.

The second policy dealt with providing a sunset of not later than seven years after the first fiscal year. In making a good-faith effort to comply, it is my intention that we will not move legislation out of this Committee that includes authorizations for a period of longer than 7 years.

My time is almost up, and I will yield back my time.

Ms. JOHNSON. No, I am going to ask unanimous consent to allow you to complete your statement.

Chairman HALL. Well, unanimous consent to allow me to complete my speech, I object.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF CHAIRMAN HALL

I am pleased to convene the markup this morning for consideration of H.R. 2096, the Cybersecurity Enhancement Act of 2011.

As our reliance on information technology expands, so do our vulnerabilities. Protecting the nation's cyber infrastructure is a responsibility shared by different Federal agencies, including the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST).

I am delighted that Congressmen McCaul and Lipinski have reintroduced the Cybersecurity Enhancement Act of 2011 which primarily addresses important cybersecurity efforts conducted by NSF and NIST.

This bill will help to support these efforts through reauthorization of activities in four general areas: (1) strategic planning for cybersecurity R&D needs across the federal government; (2) basic research at the National Science Foundation (NSF), which will hopefully increase security over the long-term; (3) enhanced NSF scholarships to increase the size and skills of the cybersecurity workforce; and (4) strengthened R&D, standards development and coordination, and public outreach at the National Institute of Standards and Technology (NIST) related to cybersecurity.

These are modest but important changes that will help us do a better job of protecting our cyber networks, and I am pleased to join as a cosponsor, along with Mr. Smith, Mr. Brooks, Mr. Wu, and Mr. Luján.

This is a good bill, and it represents a small but important step in Congress's overall efforts to address cybersecurity issues.

By strengthening agency coordination and cooperation on cybersecurity research and development efforts, this bill will help address the comprehensive cybersecurity needs of the Nation.

I want to thank Mr. McCaul and Lipinski for collaborating on this bipartisan effort, and I look forward to continued cooperative efforts as we move forward.

As long standing Members of the Science, Space, and Technology Committee know, the Committee enjoys a tradition of bipartisanship, and as evidenced by the legislation before us today, this spirit of cooperation lives on in the 112th Congress. I thank the gentleman from Texas and the gentleman from Illinois for setting an example.

It is in that spirit of cooperation, that I seek to address concerns expressed in regard to legislation taken up by this Committee.

As you are all aware, the Republican Leadership put forward legislative protocols for the 112th Congress. The protocols are intended to guide the Majority Leadership in the scheduling and consideration of legislation on the House floor.

While the protocols DO NOT govern the introduction of legislation, GOOD-FAITH compliance with the protocols will be necessary if such legislation is scheduled for the floor. In other words the protocols do not bar introduction of legislation and provide that as Committees work through the legislative process, GOOD-FAITH efforts to address and comply with the protocols can be accomplished at the Committee level.

In that vein, we have an open dialogue with Leadership on this legislation (and any legislation for that matter), as it is a priority for the Committee on both sides of the aisle.

In my remarks at our organizational meeting in February, I mentioned two policies which I wanted the Committee to abide by when considering legislation.

The first dealt with the goal that the Committee will no longer consider bills that authorize "such sums as may be necessary".

For example, the legislation in front of us today, in the previous Congress, included at least five instances of the following authorization of appropriations language, "...There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014." During the 110th and 111th Congress my Republican colleagues routinely offered amendments that eliminated the phrase "such sums as are necessary." That is the phrase which I do not want this Committee to utilize.

This is balanced with the desire to continue to provide Agencies needed flexibility within a defined amount of funding for the myriad of activities we may direct them to conduct. We continue to work through options by which to satisfy this desire.

The second policy dealt with providing a "sunset" of not later than seven (7) years after the first fiscal year spending is authorized. In making a GOOD-FAITH effort to comply, it is my intention that we will not move legislation out of this Committee that includes authorizations for a period of longer than 7 years.

For example, including specified authorization of appropriations for a program for the fiscal years 2012 through 2019 would not be permissible.

Including specified authorization of appropriations for a program for the fiscal years 2012 through 2018 would be permissible, however, it is my overall preference that we authorize for three to five year periods.

This provides programs and activities authorized to build a record from which the Committee may conduct proper oversight and legislate necessary fixes to problems sooner rather than later.

As mentioned earlier, this Committee will make a GOOD-FAITH effort to comply with the protocols, working with Members on both sides of the aisle and Leadership to craft legislation that meets the threshold necessary for floor consideration.

Bring forward your ideas, including in the form of legislation and amendments and the Committee will try its best to get those good ideas packaged in a way that permits them to be considered in the Committee and by the whole House.

I now recognize, the Ranking Member, Ms. Johnson for her opening statement.

Chairman HALL. Now, for your kindness, I am going to recognize you for five minutes, and I know you are going to comply.

Ms. JOHNSON. Thank you, Mr. Chairman.

Today, we are marking up H.R. 2096, the Cybersecurity Enhancement Act of 2011, and it really is a good bipartisan bill, nearly identical to Mr. Lipinski's bipartisan cybersecurity bill from last Congress, which moved through the Committee and passed overwhelmingly on the House floor, and I would like to thank my colleagues, Mr. Lipinski and Mr. McCaul, for their leadership and work on the bill in this Congress.

Computers, cell phones and the Internet have greatly increased our productivity and connectivity. Unfortunately, this connectivity and the dependence of our infrastructure, our commerce and a great deal of our day-to-day lives on information technologies have also increased our vulnerability to cyber attacks.

H.R. 2096 would authorize research, education and standards activities that are essential to our government's efforts to strengthen the security of our current information technology systems and to build future systems that are more secure from the outset. The two agencies covered in this bill, the National Science Foundation and the National Institute of Standards and Technology, each play an important and unique role in the federal effort to secure our cyberspace.

While H.R. 2096 is a good bill, I would be remiss if I didn't express my concern about our failure to consider this legislation through regular order. While H.R. 2096 is based in large part on legislation from last Congress, the truth is that the field of cybersecurity is rapidly evolving and two years in this field is equivalent to a lifetime in many other fields.

In addition, over the last two years, this Administration has made great strides in strengthening the government's cybersecurity efforts. As a result, some of the provisions in the bill before us today are unfortunately already out of date. The fact that we are pushing this bill through the Committee is preventing us from adequately and effectively doing our due diligence to ensure that it is as current as it should be.

I recognize that the bipartisan Manager's Amendment will make some necessary improvements and updates to the underlying bill, and I welcome these changes. I also plan to offer an amendment today that will update section 203 to reflect the current state of the National Initiative for Cybersecurity Education, and I hope my colleagues will support it.

As we mark up this bill, it is important that we consider the proposed fiscal year 2012 appropriations levels for NSF and NIST. The research accounts of both agencies would be flat-funded under the current House proposal. While flat funding might seem like a win for these agencies under the current circumstances, I think it is important that we recognize that flat funding is really declining funds when adjusted for inflation.

The Federal Government is already suffering from a lack of adequately trained cybersecurity professionals, and flat-funding these key agencies will further erode the human capital we need to build up our cybersecurity capabilities. It will also slow down much needed advances in research and development on game-changing technologies. In addition, if NIST is flat-funded, it will not be able to carry out any of the additional cybersecurity-related activities with which it has been charged over the last couple of years, including its cybersecurity education and awareness efforts, its identity management initiative, and its cloud computing security activities. It doesn't seem right to be touting NIST's role in cybersecurity while also proposing a funding level for the agency that prevents it from carrying out critical cybersecurity-related activities.

The truth is that we need to be cognizant of what these agencies will actually be able to accomplish from within the very worthy and important goals described in this legislation.

I would like to take a moment to thank the Chairman for attempting to clarify some of the issues surrounding the Majority's protocols in the 112th Congress. In recent weeks, minority Members have voiced their concerns about whether legislation moving through this Committee is consistent with the Majority's policies and protocols and whether those protocols are being properly applied to all legislation and amendments before the Committee, and while I do appreciate the Chairman's comments today, I think there are a number of unresolved issues related to the Majority's protocols that will need to be addressed before Minority Members of the Committee feel comfortable that we know the rules of the road. It is imperative that these clarifications be provided before the Committee moves with additional markups.

Thank you again, Mr. Chairman. I look forward to working with you and the rest of the Committee. I yield back.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF RANKING MEMBER JOHNSON

Thank you, Chairman Hall. Today, we are marking up H.R 2096, the *Cybersecurity Enhancement Act of 2011*. This is a good bipartisan bill, nearly identical to Mr. Lipinski's bipartisan cybersecurity bill from last Congress which moved through this Committee and passed overwhelmingly on the House floor. I would like to thank my colleagues, Mr. Lipinski and Mr. McCaul, for their leadership and work on the bill this Congress.

Computers, cell phones, and the Internet have greatly increased our productivity and connectivity. Unfortunately, this connectivity and the dependence of our infrastructure, our commerce, and a great deal of our day-to-day lives on information technologies have also increased our vulnerability to cyber attacks.

H.R. 2096 would authorize research, education, and standards activities that are essential to our government's efforts to strengthen the security of our current information technology systems and to build future systems that are more secure from the outset. The two agencies covered in this bill, the National Science Foundation and the National Institute of Standards and Technology, each play an important and unique role in the federal effort to secure our cyberspace.

While H.R. 2096 is a good bill, I would be remiss if I did not express my concern about our failure to consider this legislation through regular order. While H.R. 2096 is based in large part on legislation from last Congress, the truth is that the field of cybersecurity is rapidly evolving and two years in this field is equivalent to a lifetime in many other fields.

In addition, over the last two years, this Administration has made great strides in strengthening the government's cybersecurity efforts. As a result, some of the provisions in the bill before us today are unfortunately already out-of-date. The fact that we are rushing this bill through the Committee is preventing us from adequately and effectively doing our due diligence to ensure that it is as current as it can and should be.

I recognize that the bipartisan Manager's Amendment will make some necessary improvements and updates to the underlying bill, and I welcome these changes. I also plan to offer an amendment today that will update section 203 to reflect the current state of the National Initiative for Cybersecurity Education. I hope my colleagues will support this amendment.

There is also considerable–and growing–concern about whether legislation moving through this Committee is consistent with the Majority's policies and protocols, Unfortunately, we have not received the clarification that we have sought and are worried that the Committee is making this up as we go. In the Subcommittee markups last week, we were told that some of these authorization and funding issues would be resolved before the bills were reported out. Unfortunately, in this case, since we have come straight to Full Committee, this is our one and only bite at this apple. For the sake of Mr. McCaul and Mr. Lipinski and the other sponsors of the bill, I sure hope we've gotten it right.

Also, as we mark up this bill, it is important that we consider the proposed FY 2012 appropriations levels for NSF and NIST. The research accounts of both agencies would be flat-funded under the current House proposal. While flat-funding might seem like a "win" for these agencies under current circumstances, I think it is important that we recognize that flat funding is really declining funds when adjusted for inflation.

The federal government is already suffering from a lack of adequately trained cybersecurity professionals and flat-funding these key agencies will further erode the human capital we need to build up our cybersecurity capabilities. It will also slow down much needed advances in research and development on game-changing technologies.

In addition, if NIST is flat-funded, it will not be able to carry out any of the additional cybersecurity-related activities with which it has been charged over the last couple of years, including its cybersecurity education and awareness efforts, its identity management initiative, and its cloud computing security activities. It doesn't seem right to be touting NIST's role in cybersecurity while also proposing a funding level for the agency that prevents it from carrying out critical cybersecurity-related activities.

The truth is that we need to be cognizant of what these agencies will actually be able to accomplish from within the very worthy and important goals described in this legislation.

Thank you again, Mr. Chairman. I look forward to working with you to get this bill to the House floor. And I yield back the balance of my time.

Chairman HALL. I thank you for an exact five-minute speech, and I ask unanimous consent that my entire opening statement be

placed in the record as well as all Members' opening statements will be placed into the record at this point. Is there objection? The Chair hears none.

We will now consider the bill, H.R. 2096, the Cybersecurity Enhancement Act of 2011. I will recognize both gentlemen who handled this bill. I recognize the gentleman from Texas, Mr. McCaul, to describe the bill.

Mr. MCCAUL. Thank you, Mr. Chairman.

Let me say thank you to you and the Ranking Member for allowing us to come to the full Committee and I also want to thank my friend and colleague, Mr. Lipinski, for his great leadership and hard work on this bill. This will be the first cybersecurity bill marked up in the House of Representatives.

The cyber threat is real and it is here now. Admiral Mullen will tell you that it is one of the greatest threats that we face as a Nation today. Today's hackers are no longer thrill-seeking teenagers. They are organized crime syndicates and national militaries that commit espionage and cyber warfare from thousands of miles away. Increasingly sophisticated foreign adversaries are electronically infiltrating sensitive U.S. computer networks to obtain military technologies. They have hacked into every federal agency, including the Pentagon.

Foreign competitors and criminals unabashedly steal trade secrets from America and their companies through similar methods. There has been a huge theft of intellectual property from these countries, like China and Asia. Domestic cyber threats are increasing at an alarming rate as well. For example, one anarchist community of hackers, "Anonymous," declared war on the city of Orlando just last month. This week, 15 individuals were arrested by the FBI in the United States and five individuals were arrested in Europe for roles in cyber attacks on major U.S. companies and organizations. Critical infrastructure systems that run our financial, energy and transportation infrastructures have also become victims of cyber attacks and exploitations.

America's laws for cyberspace are decades old. We are not prepared to meet the threats of the 21st century. One reason is because we do not have a workforce readily available, and we also need to harden our federal networks from a cyber attack. That is why Congressman Lipinski and I have reintroduced the Cybersecurity Enhancement Act of 2011, which passed overwhelmingly last Congress. This act incorporates key recommendations from the Center for Strategic and International Studies report which I cochaired including improving coordination in the government. It provides for a strategic plan to assess the cybersecurity risk and guide the overall direction of federal cyber R&D. It updates the National Institute of Standards and Technology, or NIST, responsibilities to develop security standards for federal computer systems and processes for agencies to follow. It establishes a federal university-private sector taskforce to coordinate research and development. It continues much-needed cybersecurity research and development programs at the National Science Foundation and NIST. It improves training of cyber professionals, codifies scholarship programs at the National Science Foundation that can't be repaid with federal service. As I mentioned, it passed overwhelmingly last Congress. I hope we can do the same this Congress.

Most importantly, I believe that H.R. 2096 is fiscally responsible. It is not being paid for with any new money since it is intended to work within the boundaries of funds authorized and appropriated to NSF and NIST. As you may recall in the full Committee hearing we had at the end of May, witnesses from NSF, NIST, the Department of Homeland Security and the Networking Information Technology Research and Development Program all expressed their support for this bill. I am also pleased to report that the U.S. Chamber of Commerce has sent a letter of support for this bill. We have been working closely with NSF and NIST to ensure that this bill suits their needs, and I am confident that this legislation will advance the excellent work these agencies are doing regarding cybersecurity.

As we talk about threats facing the Nation, and we have many, and we are in several wars, but the idea of cyber warfare to me is one of the ideas that keeps me up at nighttime because of the devastating impact it could have on the United States. In hardening our federal networks from cyber attack from countries or from anarchists or rogue nations that want to do us harm that could cripple this Nation, bringing down our critical infrastructure. That is why this bill is so important.

I look forward to this markup and I want to thank all my colleagues for their hard work on this bill and the staff for their hard work in what I consider to be a very important piece of legislation.

With that, Mr. Chairman, I yield back.

[The prepared statement of Mr. McCaul follows:]

PREPARED STATEMENT BY REPRESENTATIVE MCCAUL

Today's hackers are no longer thrill-seeking teenagers; they are organized crime syndicates and national militaries that commit espionage. From thousands of miles away, increasingly sophisticated foreign adversaries are electronically infiltrating sensitive U.S. computer networks to obtain military technologies. Foreign competitors and criminals unabashedly steal trade secrets from American companies through similar methods.

Domestic cyber threats are increasing at an alarming rate as well. For example, one anarchic community of hackers, *Anonymous*, declared war on the city of Orlando just last month. This week, the FBI arrested 15 individuals in the U.S. and five in Europe for alleged roles in cyber attacks on major U.S. companies and organizations.

Critical Infrastructure Systems that run our financial, energy, and transportation infrastructures have also become victims of cyber attack and exploitation.

America's laws for cyberspace are decades old. We are not prepared to meet the threats of the 21st century. One reason is because we do not have a workforce readily available. That is why Congressman Lipinksi and I have reintroduced the Cybersecurity Enhancement Act of 2011.

The Cybersecurity Enhancement Act incorporates key recommendations from the Center for Strategic and International Studies (CSIS) including:

- Improves coordination in government:
  - Provides for a Strategic Plan to assess the cybersecurity risk and guide the overall direction of Federal cyber R&D
  - Updates the National Institutes of Standards and Technology (NIST) responsibilities to develop security standards for federal computer systems and processes for agencies to follow
- Establishes a federal-university-private-sector task force to coordinate research and development.
- Continues much needed cybersecurity research and development programs at the National Science Foundation and the National Institute of Standards and Technology.
- Improves training of cyber professionals. Codifies scholarship programs at the National Science Foundation (NSF) that can be repaid with federal service.

Through a bipartisan effort, this bill passed last Congress (422-5). I hope to see this bill successfully passes again and to work with my friends across the aisle on much needed future cybersecurity initiatives.

Most importantly, H.R. 2096 is fiscally responsible. It is not being paid with any new money since it is intended to work within the boundaries of funds authorized and appropriated to NSF and NIST.

As you may recall in the Full Committee Hearing we had at the end of May, witnesses from NSF, NIST, the Department of Homeland Security (DHS), and the Networking and Information Technology Research and Development Program expressed their support for the bill. The US Chamber of Commerce has also sent a letter of support. We have been working closely with NSF and NIST to ensure this bill suits their needs. I'm confident that this legislation will advance the excellent work these agencies are doing regarding cyber security.

Chairman HALL. Thank you. The gentleman yields back.

I recognize the gentleman from Illinois, Mr. Lipinski, for his statement on the bill.

Mr. LIPINSKI. I thank you, Chairman Hall, and I want to thank you and Ranking Member Johnson for holding this markup on a bill that is certainly a priority for me, and it is an issue that must be a priority for our Nation.

I hope that we can all work together to advance this important cybersecurity research and education bill to help our Nation counter the numerous cyber threats that attack federal and military IT systems every day as well as the private sector.

I would like to thank Mr. McCaul for his work in taking the lead as we reintroduced this bill in this Congress. In 2009, our roles were reversed and we worked together to advance this legislation through the House where it passed on a 422–5 vote. Unfortunately, like far too many pieces of legislation, it was not taken up in the Senate, but it is my hope that by advancing this bill now and working with Senator Menendez, who has introduced a companion measure this Congress, we can get this passed into law, perhaps as part of a comprehensive cybersecurity bill.

We have all seen much too much evidence demonstrating why this legislation is needed. It is clear that our adversaries are working tirelessly to exploit weaknesses in the IT systems of our military, government as well as the private sector. Take for instance the recently disclosed cyber attacks against our military. In March of this year, an astonishing 24,000 Pentagon files were stolen during a major breach. An assault that Deputy Defense Secretary Lynn called "the most damaging cyber attack to date on the military."

I am equally troubled that the Deputy Secretary's revelation that over the last decade terabytes of data have been stolen by foreign intruders from the corporate networks of defense companies. The thefts include information concerning some of our most sensitive systems including avionics, satellites, and network security protocols.

The severity of this ever-evolving threat is clear. We must do all we can to arm our workforce and all Americans who are online with the most up-to-date research and technology that will enable us to build a cybersecurity program that is second to none, a program that protects our critical infrastructure, the Federal Government's computer networks, our troops and, most of all, all of the American people.

The legislation we are considering today focuses on three areas where the NSF and NIST have already established programs in re-

search, education, and standards. It includes the development and implementation of a risk-based strategic plan for federal R&D, the forging of partnerships with universities and industry that explore mechanisms for carrying out collaborative research in cybersecurity, and a program aimed at increasing public awareness of cyber risk by requiring NIST to develop a plan for examining best practices and technical standards to the general public in a user-friendly format that will improve their basic cybersecurity knowledge. And I think this is one of the most overlooked pieces, and the hearings that we had in the last Congress pointed out that computer hygiene is incredibly important and is one of the biggest weaknesses that we have right now in cybersecurity.

The legislation also contains a number of critical education programs designed to train the cybersecurity workers of our Nation in what businesses need. It pays particular attention to the workforce needs of the Federal Government by providing NSF fellowships to students pursuing advanced degrees in cybersecurity-related fields and scholarships for service program for students that agree to repay taxpayers for their education through service in the Federal Government.

I believe it is a good bill that deserves the bipartisan support it received last Congress. I hope we can continue to build on the progress we made last year and my colleagues will join Mr. McCaul and me to pass this important component of our Congressional response to America's cyber challenges.

I thank you, Chairman Hall, and I yield back the balance of my time.

Chairman HALL. The gentleman yields back.

At this time, does anyone else wish to comment on the bill? If not, without objection I ask unanimous consent that the bill is considered as read and open to amendment at any point and that Members proceed with amendments. Is there objection? The Chair hears none.

The bill is now open for amendments. Are there any amendments to the bill?

Mr. MCNERNEY. Mr. Chairman, I have an amendment at the desk.

Mr. MCCAUL. Mr. Chairman.

Chairman HALL. The first amendment on the roster is offered by Mr. McCaul, which is supported by Mr. Lipinski. The clerk shall report the amendment.

The CLERK. Amendment number 024, amendment to H.R. 2096, offered by Mr. McCaul of Texas.

[The amendment appears in the Appendix]

Chairman HALL. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

I recognize the gentleman for five minutes to explain his amendment.

Mr. MCCAUL. Thank you, Mr. Chairman.

The Manager's Amendment makes minor clarifications to the cybersecurity university-industry task force section and makes some technical changes to the bill, but primarily it updates several provisions specific to the National Institute of Standards and Technology's activities in cybersecurity. Many of these changes were based upon feedback provided to us by NIST and are designed to

update technical language and activities that have changed since this bill was originally introduced in the 111th Congress.

Specifically, the amendment updates the activities related to NIST's creation and dissemination of computer security checklists. These checklists are an important part of ensuring that federal agencies have a standard process to reference when they are making sure their hardware and software systems are as secure as possible. The amendment updates language originally provided in the Cybersecurity Research and Development Act of 2002, ensuring that the technical wording reflects the current state of art which has advanced to include more automated procedures.

Next, the amendment clarifies that federal agency involvement in the development of international cybersecurity standards should be coordinated amongst the agencies. NIST is tasked with working with other agencies and private sector stakeholders involved in standards development. The amendment improves the language in the earlier version of the bill by clarifying that government representation is not mandatory and ensuring the involvement of non-governmental stakeholders. NIST is also required to report to the Congress on the coordination efforts.

This amendment also updates language regarding cybersecurity awareness and education activities at NIST by clarifying that NIST will continue to coordinate these activities with other agencies with shared responsibilities. For example, part of the National Science Foundation's cybersecurity efforts support many college students who may ultimately serve in the federal workforce, so this part of the amendment supports NIST continuing to utilize their expertise and standards and best practices. It also requests a strategic plan and report to Congress so we can keep track and oversight of what all the different agencies are doing and spending on cybersecurity awareness and education.

And last but not least, the amendment includes language articulating that this bill is intended to work within the boundaries of funds authorized and appropriated to NIST. The language helps clarify that we are not expanding the authorized amounts for NIST research activities but rather highlighting some areas important to cybersecurity that should be included in the work they conduct within their research and development budget.

Let me again thank Mr. Lipinski for working closely with me on the components of this Manager's Amendment, and I appreciate his strong support in making these important updates. Though the previous language was good, I believe that this amendment makes it even better. And with that, Mr. Chairman, I yield back.

PREPARED STATEMENT BY REPRESENTATIVE MCCAUL TO H.R. 2096

Thank you, Mr. Chairman.

The Manager's Amendment makes minor clarifications to the Cybersecurity University-Industry Task Force section and makes some technical changes to the bill, but primarily, it updates several provisions specific to the National Institute of Standards and Technology (NIST) activities in cybersecurity. Many of these changes were based on feedback provided by NIST, and are designed to update technical language and activities that have changed since this bill was originally introduced in the 111th Congress.

Specifically, the amendment updates the activities related to NIST's creation and dissemination of computer security checklists. These checklists are an important part of ensuring that Federal agencies have a standard process to reference when they are making sure their hardware and software systems are as secure as possible.

The amendment updates language originally provided in the Cyber Security Research and Development Act of 2002, ensuring that the technical wording reflects the current state of the art, which has advanced to include more automated procedures.

Next, the amendment clarifies that Federal agency involvement in the development of international cybersecurity standards should be coordinated amongst the agencies. NIST is tasked with working with other agencies and private sector stakeholders involved in standards development.

The amendment improves on the language in the earlier version of the bill by clarifying that government representation is not mandatory, and ensuring the involvement of non-governmental stakeholders. NIST is also required to report to Congress on the coordination efforts.

The amendment also updates language regarding cybersecurity awareness and education activities at NIST by clarifying that NIST will continue to coordinate these activities with other agencies with shared responsibilities. For example, part of the National Science Foundation's cybersecurity efforts support many college students who may ultimately serve in the federal workforce. So, this part of the amendment supports NIST continuing to utilize their expertise in standards and best practices, and also requests a strategic plan and report to Congress so we can keep track of what all of the different agencies are doing and spending on cybersecurity awareness and education.

Last but not least, the amendment includes language articulating that this bill is intended to work within the boundaries of funds authorized and appropriated to NIST. The language included helps clarify that we are not expanding the authorized amounts for NIST's research activities, but rather highlighting some areas important to cybersecurity that should be included in the work they conduct within their research and development budget.

I thank Mr. Lipinski for working closely with me on the components of this manager's amendment and appreciate his support in making these important updates. Though the previous language was good, I believe this amendment makes it even better.

Chairman HALL. The gentleman yields back. I want to thank the gentleman for the amendment. I support the amendment.

Is there further discussion on the amendment? Mr. Lipinski.

Mr. LIPINSKI. Yes, Mr. Chairman. Move to strike the last word.

Chairman HALL. I recognize you for five minutes.

Mr. LIPINSKI. Thank you. I will be very quick.

I want to express my appreciation for Mr. McCaul's willingness to work together on these changes. I am very pleased the Manager's Amendment incorporates feedback from both sides of the aisle. Mr. McCaul did a very good job of going through what these changes are. There are a couple sections, though, that I wanted to talk about.

The amendment modifies the cybersecurity awareness and education language in section 203 to require a strategic plan and report to Congress. I strongly support these modifications and appreciate their inclusion. However, I do wish that we had been able to find a bipartisan agreement on language that would have been more representative of the current National Initiative on Cyber Security Education program, the NICE program, that NIST coordinates and oversees, and I hope that we continue to work together on this matter as we move forward.

In addition, the Management's Amendment includes a new section 205 to specify the source of authorizations. I recognize that there are still questions about how bills and amendments need to be drafted to comply with the Majority's new policies and protocols. However, I am not entirely confident that this language provides the clarity sought by some of my colleagues and I hope that this also is an area we can continue to work together on as we advance this bill. I am sure that we can continue as we move forward on this to work together.

I want to thank Mr. McCaul for all that he has done. I think this Manager's Amendment makes some needed improvements to the bill, and I will yield back.

Chairman HALL. The gentleman yields back.

Are there any other comments at this time? Are there any amendments to the amendment offered by the gentleman from Texas and the gentleman from Illinois?

Mr. MCNERNEY. Mr. Chairman, I have an amendment at the desk.

Chairman HALL. The clerk will report the amendment.

The CLERK. Amendment number 025, amendment to H.R. 2096, offered by Mr. McNerney of California to the amendment offered by Mr. McCaul of Texas.

[The amendment appears in the Appendix]

Chairman HALL. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

The gentleman is recognized for five minutes to explain his amendment.

Mr. MCNERNEY. Thank you, Mr. Chairman. I want to thank you for bringing this bill forward and Mr. McCaul and Mr. Lipinski for their hard work to advance the cybersecurity capability of this Nation within the jurisdiction of this Committee.

The amendment I offer today is a straightforward and non-controversial proposal. My amendment simply ensures that our national laboratories are able to contribute their expertise as we research and develop the standards to enhance cybersecurity.

Specifically, my amendment adds national laboratories to the list of entities that should contribute to the cybersecurity education and awareness program. Two of our national labs operate facilities located in Livermore, California, and employ many of my constituents. The labs and their employees are working tirelessly on issues that further our national security and our national research needs. Our national labs are making important contributions to the development of cybersecurity technology and defenses, and I am confident that they will make important contributions to the education and awareness campaign.

For instance, Sandia National Laboratories established the Center for Cyber Defenders over a decade ago. The Cyber Defenders program allows computer science students to gain practical experience in the realm of computer operations, network protection and information systems. By working with experts in the field, these students will better understand how to focus their education in real-life situations.

Cybersecurity is a broad field that is constantly evolving, and promoting national cybersecurity awareness and education is an important goal. Our national laboratories and programs like the Cyber Defenders can be an important part of our efforts.

I urge my colleagues to support my amendment and the role of our national labs in the field of cybersecurity. I yield back.

Chairman HALL. The gentleman yields back, and I thank the gentleman for his amendment including the national laboratories to cybersecurity education and awareness for them to coordinate together. I support the amendment.

If there are no further Members wishing to be recognized, the vote will occur on the amendment. Are there any other discussions

on the amendment? The Chair hears none. All in favor, say aye. Those opposed, no. The ayes have it and the amendment is agreed to.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 **AMENDMENT NO. 025** **ROLL CALL NO._____**

Bill: H. R. 2096

SPONSOR: Mr. McNerney

Agreed To By Voice Vote

Quorum –14 to vote –21 to report

MEMBER	AYE	NO	PRESENT	NOT VOTING
1 Mr. HALL, *Chair* - *TX*				
2 Mr. SENSENBRENNER – *WI* **				
3 Mr. SMITH - *TX*				
4 Mr. ROHRABACHER - *CA*				
5 Mr. BARTLETT - *MD*				
6 Mr. LUCAS - *OK*				
7 Mrs. BIGGERT - *IL*				
8 Mr. AKIN - *MO*				
9 Mr. NEUGEBAUER - *TX*				
10 Mr. McCAUL - *TX*				
11 Mr. BROUN - *GA*				
12 Mrs. ADAMS - *FL*				
13 Mr. QUAYLE - *AZ*				
14 Mr. FLEISCHMANN - *TN*				
15 Mr. RIGELL - *VA*				
16 Mr. PALAZZO - *MS*				
17 Mr. BROOKS - *AL*				
18 Mr. HARRIS - *MD*				
19 Mr. HULTGREN - *IL*				
20 Mr. CRAVAACK - *MN*				
21 Mr. BUCSHON - *IN*				
22 Mr. BENISHEK - *MI*				
23 Vacancy				
1 Ms. JOHNSON, *Ranking* - *TX*				
2 Mr. COSTELLO - *IL*				
3 Ms. WOOLSEY - *CA*				
4 Ms. LOFGREN - *CA*				
5 Mr. WU - *OR*				
6 Mr. MILLER - *NC*				
7 Mr. LIPINSKI - *IL*				
8 Ms. GIFFORDS - *AZ*				
9 Ms. EDWARDS - *MD*				
10 Ms. FUDGE - *OH*				
11 Mr. LUJÁN - *NM*				
12 Mr. TONKO - *NY*				
13 Mr. McNERNEY - *CA*				
14 Mr. SARBANES - *MD*				
15 Ms. SEWELL - *AL*				
16 Ms. WILSON - *FL*				
17 Mr. CLARKE - *MI*				
TOTALS				

** Vice Chair

Are there any other amendments to the amendment?

Ms. JOHNSON. Mr. Chairman, I have an amendment at the desk.

Chairman HALL. The clerk will report the amendment.

The CLERK. Amendment number 040, amendment offered by Ms. Eddie Bernice Johnson of Texas to the amendment offered by Mr. McCaul of Texas.

[The amendment appears in the Appendix]

Chairman HALL. I ask unanimous consent to dispense with the reading. Without objection, it is so ordered.

The gentlewoman is recognized for five minutes to explain her amendment.

Ms. JOHNSON. Thank you very much, Mr. Chairman.

My amendment today is really very simple. It seeks to update section 203 of the Manager's Amendment to ensure that the activities authorized are reflective of the current National Initiative for Cybersecurity Education, or NICE.

Right now, the Manager's Amendment identifies two activities on the NIST awareness and education program, the widespread dissemination of cybersecurity technical standards and best practices; and efforts to make technical standards and best practices more usable by individuals and small businesses. While these important activities are ones that NIST should continue to pursue, they do not adequately depict the activities being carried out under NICE. In fact, none of the activities authorized under section 203 explicitly mentions education or public awareness activities. I don't believe my colleagues are intending to change the scope of the existing initiative, but if we are going to authorize the cybersecurity awareness and education initiative at NIST, then it makes sense to ensure that we are accurately representing the current scope of work. And that is what my amendment does.

Finding qualified personnel to fill cybersecurity positions across the Federal Government remains a challenge. For example, in 2010, DHS set the goal of hiring 1,000 cybersecurity professionals over three years, but to date, they have only hired approximately 200. Additionally, a recent report by the Department of Justice Inspector General found that FBI field agents lack the network and counterintelligence expertise to investigate national security intrusions effectively. Not only are federal agencies competing with the private sector for qualified personnel, but they are also competing with each other for these individuals. The success of NICE is essential and it will go a long ways to ensuring that we have the cybersecurity personnel necessary to keep individuals and companies safe online.

I urge adoption of this amendment and yield back the balance of my time.

Chairman HALL. The gentlelady yields back the balance of her time.

It has to be noted, and it is my understanding that this amendment has been revised and we only received the revision an hour before the markup today, or right around 9:00, and while I am certain that the gentlelady is trying to improve her amendment to make the program better, we can't consider the change on such short notice because Members and staff have not had adequate time to examine the proposal.

If the Ranking Member would withdraw her amendment, I would be very happy to work with her as this bill moves forward.

Ms. JOHNSON. Thank you, Mr. Chairman. I would like to comment on that.

The only change that was made, we got word that you would object if we removed the existing language and substitute. What we did was simply not remove the existing language and added the other points to it that were already constructed as amendments.

Chairman HALL. I yield the gentlelady another five minutes to discuss her amendment.

Ms. JOHNSON. Okay. The only thing we did, we had made it a point to upgrade the amendment to current level of functioning by eliminating the first two statements that were made related. When we got the word that there was an objection to eliminating those two paragraphs or phrases, we simply added them back, didn't take them out and added the updated language to that. We are just trying to make sure that when we pass this bill, it is not already outdated.

Chairman HALL. Is there further discussion on the amendment to the amendment?

Mr. MCCAUL. Mr. Chairman.

Chairman HALL. Who seeks recognition?

Mr. MCCAUL. Mr. McCaul.

Chairman HALL. Mr. McCaul, I recognize you for five minutes.

Mr. MCCAUL. Let me just say first to the Ranking Member, I want to commend you. This is a very, very important issue. I think as Mr. Lipinski pointed out, the cyber education and awareness piece, the computer hygiene, when you talk to NSA, they will tell you that is about 85 percent of what we need to do to protect our networks. And so I know that the Chairman is concerned that there is some last-minute vetting that needs to be done and maybe talking to some of the stakeholders but I look forward to working with you. I think this can be—I think we can reach a solution here so that we can get this language in the final draft of the bill.

And so with that, I yield back.

Chairman HALL. The gentleman yields back, and there is still an issue with the amendment being redundant, something that could probably be worked out, but the gentlelady has her right to make further answer or I will recognize anyone else to be heard on this.

Ms. JOHNSON. I simply want to thank the gentleman, Mr. Chairman, and to thank you. I really don't know what to say. All I am trying to do is update the language. All we did when we found there was objection to removing the outdated language, we decided we could leave the outdated language there and just add the updated language so it would be current, and that is all this amendment does. I will be happy to work with Mr. McCaul because I want his bill to be the best we can offer and it won't look like we didn't check to see that it was already outdated.

Chairman HALL. Do you yield back?

Ms. JOHNSON. I yield back.

Chairman HALL. Do you wish to withdraw the amendment and work with the two sponsors of it as we go? I want to give you every opportunity to do that.

Ms. JOHNSON. Yes, I will withdraw it, as long as it is incorporated when it goes out of full Committee so that we don't look like fools with language that is already outdated.

Chairman HALL. I can't assure you we won't look like fools but I think that we could either have a vote on it or you withdraw it. I hope you will withdraw it.

Ms. JOHNSON. Well, let me just have some assurance. Before we go to the floor, will this opportunity exist? I am not trying to make the bill worse. I am not trying to destroy the bill. I am trying to make it look like we know what we are doing by sending out language where we are currently.

Chairman HALL. I think the amendment speaks for itself. I want to work with you before it goes to the floor.

Ms. JOHNSON. Well, thank you.

Chairman HALL. It goes to the floor after we adjourn today.

Ms. JOHNSON. Well, at what point was Mr. McCaul talking about working with me? I will be happy to do that.

Mr. MCCAUL. Mr. Chairman?

Chairman HALL. Yes, sir. I recognize Mr. McCaul.

Mr. MCCAUL. I do think that the gentlelady—this is an important issue, an important part of the bill that I think we want to make it as updated as possible and so I am very willing to work with the Ranking Member to perfect this language. We got this so late that we want to vet it some more, but certainly it could be added in a Manager's Amendment on the floor, and I think we are going to have probably some other amendments that we will probably do the same thing. So I don't know if the Ranking Member——

Ms. JOHNSON. Thank you. That is adequate for me. Like I indicated earlier, the first amendment simply removed the outdated language and added the new language. When we changed it, what you call the quick language, all we did was not remove the outdated language and added to it the updated language. I don't have any pride of waiting. I just want to make sure that when the bill does hit the floor, perhaps it will include the updated language as it should be, coming from a Committee of intelligence, people with supposed intelligence. Thank you.

Chairman HALL. I guess because of the protocols that leadership has put on this Committee and put on this Chairman, if you don't withdraw it, we will have a vote on it. If you do withdraw it, it is my belief that the two authors of this bill would surely go to Rules and ask that it be considered favorably, and if they assured you of that, would that help you in your withdrawal?

Ms. JOHNSON. Yes, sir.

Chairman HALL. Alright.

Ms. JOHNSON. I just want the record to reflect that if this goes to the floor without this language, don't count me as one of who didn't know better. Thank you.

Chairman HALL. We will count you however you—but right now we have to count this Committee. You have withdrawn your amendment?

Ms. JOHNSON. Yes.

Chairman HALL. The gentlelady withdraws her amendment.

Is there any other discussion on the amendment?

Mr. LUJÁN. Mr. Chairman?

Chairman HALL. Who seeks recognition?

Mr. LUJÁN. Over here, Luján.

Chairman HALL. Mr. Luján.

Mr. LUJÁN. Thank you, Mr. Chairman, and again, I appreciate you bringing this to the floor. I have an amendment at the desk.

Chairman HALL. We are going to stay here until we do that, but we are not quite ready for that yet. We will get to you in just a minute.

Is there further discussion on the amendment offered by the gentlelady or on the bill itself from the gentleman from Texas?

The vote will be on Mr. McCaul's amendment as amended. All those in favor, say aye. Opposed, no. The ayes have it and the amendment is amended and is agreed to.

Are there any other amendments?

Mr. BARTLETT. Mr. Chairman?

Chairman HALL. Who seeks recognition?

Mr. BARTLETT. Here.

Chairman HALL. Mr. Bartlett is recognized for five minutes.

Mr. BARTLETT. Mr. Chairman, I understand that the Majority is willing to accept six of the following amendments. Is that correct?

Chairman HALL. I will have to check on that. I know we do four; I am not sure six.

Mr. BARTLETT. My understanding is that the Majority is willing to accept Luján 030, Luján 032, Luján 033, Smith 042, Fudge 027 and Lipinski 032. Am I correct?

Chairman HALL. You are correct if that adds up to six.

Mr. BARTLETT. Do the Committee rules preclude considering amendments en bloc?

Chairman HALL. It will take a unanimous consent.

Mr. BARTLETT. Then may I make a unanimous consent that we consider the six amendments that the Majority is willing to accept en bloc?

Chairman HALL. Is there objection? The Chair hears none. So ordered.

Is there objection? Does everyone agree to adoption of the amendments en bloc? Is there objection? The Chair hears none. They are adopted and it is passed.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 AMENDMENT NO. 024 ROLL CALL NO._____

Bill: H. R. 2096
SPONSOR: Mr. McCaul

Agreed To By Voice Vote

Quorum –14 to vote –21 to report

MEMBER	AYE	NO	PRESENT	NOT VOTING
1 Mr. HALL, *Chair* - TX				
2 Mr. SENSENBRENNER – WI **				
3 Mr. SMITH - TX				
4 Mr. ROHRABACHER - CA				
5 Mr. BARTLETT - MD				
6 Mr. LUCAS - OK				
7 Mrs. BIGGERT - IL				
8 Mr. AKIN - MO				
9 Mr. NEUGEBAUER - TX				
10 Mr. McCAUL - TX				
11 Mr. BROUN - GA				
12 Mrs. ADAMS - FL				
13 Mr. QUAYLE - AZ				
14 Mr. FLEISCHMANN - TN				
15 Mr. RIGELL - VA				
16 Mr. PALAZZO - MS				
17 Mr. BROOKS - AL				
18 Mr. HARRIS - MD				
19 Mr. HULTGREN - IL				
20 Mr. CRAVAACK - MN				
21 Mr. BUCSHON - IN				
22 Mr. BENISHEK - MI				
23 Vacancy				
1 Ms. JOHNSON, *Ranking* - TX				
2 Mr. COSTELLO - IL				
3 Ms. WOOLSEY - CA				
4 Ms. LOFGREN - CA				
5 Mr. WU - OR				
6 Mr. MILLER - NC				
7 Mr. LIPINSKI - IL				
8 Ms. GIFFORDS - AZ				
9 Ms. EDWARDS - MD				
10 Ms. FUDGE - OH				
11 Mr. LUJÁN - NM				
12 Mr. TONKO - NY				
13 Mr. McNERNEY - CA				
14 Mr. SARBANES - MD				
15 Ms. SEWELL - AL				
16 Ms. WILSON - FL				
17 Mr. CLARKE - MI				
TOTALS				

** Vice Chair

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 AMENDMENT NO. 030 ROLL CALL NO._____

Bill: H. R. 2096
SPONSOR: Mr. Lujan

Agreed to in EnBloc
Amendments 1 of 6

Quorum –14 to vote –21 to report

MEMBER	AYE	NO	PRESENT	NOT VOTING
1 Mr. HALL, *Chair* - TX				
2 Mr. SENSENBRENNER – WI **				
3 Mr. SMITH - TX				
4 Mr. ROHRABACHER - CA				
5 Mr. BARTLETT - MD				
6 Mr. LUCAS - OK				
7 Mrs. BIGGERT - IL				
8 Mr. AKIN - MO				
9 Mr. NEUGEBAUER - TX				
10 Mr. McCAUL - TX				
11 Mr. BROUN - GA				
12 Mrs. ADAMS - FL				
13 Mr. QUAYLE - AZ				
14 Mr. FLEISCHMANN - TN				
15 Mr. RIGELL - VA				
16 Mr. PALAZZO - MS				
17 Mr. BROOKS - AL				
18 Mr. HARRIS - MD				
19 Mr. HULTGREN - IL				
20 Mr. CRAVAACK - MN				
21 Mr. BUCSHON - IN				
22 Mr. BENISHEK - MI				
23 Vacancy				
1 Ms. JOHNSON, *Ranking* - TX				
2 Mr. COSTELLO - IL				
3 Ms. WOOLSEY - CA				
4 Ms. LOFGREN - CA				
5 Mr. WU - OR				
6 Mr. MILLER - NC				
7 Mr. LIPINSKI - IL				
8 Ms. GIFFORDS - AZ				
9 Ms. EDWARDS - MD				
10 Ms. FUDGE - OH				
11 Mr. LUJÁN - NM				
12 Mr. TONKO - NY				
13 Mr. McNERNEY - CA				
14 Mr. SARBANES - MD				
15 Ms. SEWELL - AL				
16 Ms. WILSON - FL				
17 Mr. CLARKE - MI				
TOTALS				

** Vice Chair

PREPARED STATEMENT OF REPRESENTATIVE LUJÁN

Thank you Mr. Chairman. I also want to commend Congressman McCaul and Congressman Lipinski for their work on this important legislation, which I am proud to cosponsor.

Americans today are increasingly relying on the internet for essential, everyday activities. We do our banking online. We pay our taxes online, apply for jobs online and purchase clothing and groceries online. People use the internet to network and connect with family and friends. And as our dependence on internet technology and commerce to conduct daily activities continues to increase, more and more Americans are relying on secure networks to keep their personal information safe.

Abuse of personal data obtained through the internet is a real problem that can have devastating consequences. Americans should feel confident that their personal data is protected and that they are not at risk of identity theft or other abuses of consumer information.

My amendment ensures that a focus on consumer privacy is included in the Cyber Security Strategic Research and Development Plan in Section 103.

As we develop a federal strategy to combat harmful cyber attacks and establish a cybersecurity R&D plan, it is imperative that protecting consumer privacy is a top priority. I encourage my colleagues to support this amendment and I urge its adoption.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 AMENDMENT NO. 032 ROLL CALL NO._____

Bill: H. R. 2096
SPONSOR: Mr. LuJan

Agreed to in EnBloc
Amendments 2 of 6

Quorum –14 to vote –21 to report

MEMBER	AYE	NO	PRESENT	NOT VOTING
Mr. HALL, *Chair* - *TX*				
Mr. SENSENBRENNER – *WI* **				
Mr. SMITH - *TX*				
Mr. ROHRABACHER - *CA*				
Mr. BARTLETT - *MD*				
Mr. LUCAS - *OK*				
Mrs. BIGGERT - *IL*				
Mr. AKIN - *MO*				
Mr. NEUGEBAUER - *TX*				
Mr. McCAUL - *TX*				
Mr. BROUN - *GA*				
Mrs. ADAMS - *FL*				
Mr. QUAYLE - *AZ*				
Mr. FLEISCHMANN - *TN*				
Mr. RIGELL - *VA*				
Mr. PALAZZO - *MS*				
Mr. BROOKS - *AL*				
Mr. HARRIS - *MD*				
Mr. HULTGREN - *IL*				
Mr. CRAVAACK - *MN*				
Mr. BUCSHON - *IN*				
Mr. BENISHEK - *MI*				
Vacancy				
Ms. JOHNSON, *Ranking* - *TX*				
Mr. COSTELLO - *IL*				
Ms. WOOLSEY - *CA*				
Ms. LOFGREN - *CA*				
Mr. WU - *OR*				
Mr. MILLER - *NC*				
Mr. LIPINSKI - *IL*				
Ms. GIFFORDS - *AZ*				
Ms. EDWARDS - *MD*				
Ms. FUDGE - *OH*				
Mr. LUJÁN - *NM*				
Mr. TONKO - *NY*				
Mr. McNERNEY - *CA*				
Mr. SARBANES - *MD*				
Ms. SEWELL - *AL*				
Ms. WILSON - *FL*				
Mr. CLARKE - *MI*				
TOTALS				

** Vice Chair

PREPARED STATEMENT OF REPRESENTATIVE LUJÁN

Thank you Mr. Chairman. The cybersecurity threat is rapidly evolving; changes take place on a fast time scale. In recognition of this I offer this amendment to Section 103 to emphasize that the required cybersecurity research and development plan should be structured so that R&D is *rapidly* transferred into new cybersecurity technologies for the *timely* benefit of society. Federal R&D agencies are not well known for their quick turnaround time and so I think it is appropriate to highlight the need for a fast-paced program in the legislation. This amendment only adds the two words "rapid" and "timely" to the bill and so it does not make a substantial change. However, I think it is a useful addition to help the R&D keep pace with the rapidly evolving cybersecurity threat, and I urge its adoption.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 AMENDMENT NO. 033 ROLL CALL NO.____

Bill: H. R. 2096
SPONSOR: Mr. Lujan

Agreed to in EnBloc
Amendments 3 of 6

Quorum –14 to vote –21 to report

	MEMBER	AYE	NO	PRESENT	NOT VOTING
1	Mr. HALL, ***Chair*** - TX				
2	Mr. SENSENBRENNER – WI **				
3	Mr. SMITH - TX				
4	Mr. ROHRABACHER - CA				
5	Mr. BARTLETT - MD				
6	Mr. LUCAS - OK				
7	Mrs. BIGGERT - IL				
8	Mr. AKIN - MO				
9	Mr. NEUGEBAUER - TX				
10	Mr. McCAUL - TX				
11	Mr. BROUN - GA				
12	Mrs. ADAMS - FL				
13	Mr. QUAYLE - AZ				
14	Mr. FLEISCHMANN - TN				
15	Mr. RIGELL - VA				
16	Mr. PALAZZO - MS				
17	Mr. BROOKS - AL				
18	Mr. HARRIS - MD				
19	Mr. HULTGREN - IL				
20	Mr. CRAVAACK - MN				
21	Mr. BUCSHON - IN				
22	Mr. BENISHEK - MI				
23	Vacancy				
1	Ms. JOHNSON, ***Ranking*** - TX				
2	Mr. COSTELLO - IL				
3	Ms. WOOLSEY - CA				
4	Ms. LOFGREN - CA				
5	Mr. WU - OR				
6	Mr. MILLER - NC				
7	Mr. LIPINSKI - IL				
8	Ms. GIFFORDS - AZ				
9	Ms. EDWARDS - MD				
10	Ms. FUDGE - OH				
11	Mr. LUJÁN - NM				
12	Mr. TONKO - NY				
13	Mr. McNERNEY - CA				
14	Mr. SARBANES - MD				
15	Ms. SEWELL - AL				
16	Ms. WILSON - FL				
17	Mr. CLARKE - MI				
	TOTALS				

** Vice Chair

PREPARED STATEMENT OF REPRESENTATIVE LUJÁN

Thank you Mr. Chairman. This is a very simple amendment. It adds National Labs to the list of entities to consult when developing the required cybersecurity strategic research and development plan in Section 103. National laboratories are conducting groundbreaking cybersecurity research and regularly work with the private sector as well as national security agencies. They are therefore a valuable resource and worthy of being added to the list of those to consult when developing the strategic plan. I urge the adoption of this amendment.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 AMENDMENT NO. 042 ROLL CALL NO.____

Bill: H. R. 2096
SPONSOR: Mr. Smith

Agreed to in EnBloc
Amendments 4 of 6

Quorum –14 to vote –21 to report

MEMBER	AYE	NO	PRESENT	NOT VOTING
1 Mr. HALL, *Chair* - TX				
2 Mr. SENSENBRENNER – WI **				
3 Mr. SMITH - TX				
4 Mr. ROHRABACHER - CA				
5 Mr. BARTLETT - MD				
6 Mr. LUCAS - OK				
7 Mrs. BIGGERT - IL				
8 Mr. AKIN - MO				
9 Mr. NEUGEBAUER - TX				
10 Mr. McCAUL - TX				
11 Mr. BROUN - GA				
12 Mrs. ADAMS - FL				
13 Mr. QUAYLE - AZ				
14 Mr. FLEISCHMANN - TN				
15 Mr. RIGELL - VA				
16 Mr. PALAZZO - MS				
17 Mr. BROOKS - AL				
18 Mr. HARRIS - MD				
19 Mr. HULTGREN - IL				
20 Mr. CRAVAACK - MN				
21 Mr. BUCSHON - IN				
22 Mr. BENISHEK - MI				
23 Vacancy				
1 Ms. JOHNSON, *Ranking* - TX				
2 Mr. COSTELLO - IL				
3 Ms. WOOLSEY - CA				
4 Ms. LOFGREN - CA				
5 Mr. WU - OR				
6 Mr. MILLER - NC				
7 Mr. LIPINSKI - IL				
8 Ms. GIFFORDS - AZ				
9 Ms. EDWARDS - MD				
10 Ms. FUDGE - OH				
11 Mr. LUJÁN - NM				
12 Mr. TONKO - NY				
13 Mr. McNERNEY - CA				
14 Mr. SARBANES - MD				
15 Ms. SEWELL - AL				
16 Ms. WILSON - FL				
17 Mr. CLARKE - MI				
TOTALS				

** Vice Chair

PREPARED STATEMENT OF REPRESENTATIVE SMITH

Thank you, Mr. Chairman, for considering my amendment to this important piece of legislation to secure the digital domain.

My hometown of San Antonio is often referred to as ″Cyber-City USA″ due to the relevant work of the Air Force, universities and industry. Having recently received Top Secret briefings on America's cybersecurity threat, I know this legislation is timely and urgent.

At hearings before this Committee, cybersecurity experts expressed serious concerns that America faces a significant shortage of trained professionals who are skilled at countering various cyber crimes and threats.

H.R. 2096 requires the president to make an assessment of the technical workforce needs for the federal government. My amendment expands the scope of this assessment to include State and local entities, because they face cyber threats as well.

For example, two years ago, a computer virus shut down the City of Houston's municipal court for several days. And last month, hackers perpetrated a denial-of-service internet attack against the city of Orlando, Florida.

H.R. 2096 also establishes a White House-led cybersecurity task force with universities and industry to better organize America's Research and Development efforts. Since education and training for a technically-trained workforce is a challenge for all members of this consortium, my amendment directs this task force to explore ways to better leverage each other's work in training cyber professionals.

My hope, which Committee staff assures me can be addressed in the bill's report, is that this task force will consider traditional education, as well as outside-the-classroom training. Competitions, simulations and exercises like those conducted by the privately-funded US Cyber Challenge and Cyber-Patriot competitions for high school and college students provide hands-on, real world experience.

This amendment will complement a good bill that helps harness America's technical talent to address a pressing need in the cyber domain.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 AMENDMENT NO. 027 ROLL CALL NO._____

Bill: H. R. 2096
SPONSOR: Ms. Fudge

Agreed to in EnBloc
Amendments 5 of 6

Quorum –14 to vote –21 to report

	MEMBER	AYE	NO	PRESENT	NOT VOTING
1	Mr. HALL, *Chair* - TX				
2	Mr. SENSENBRENNER – WI **				
3	Mr. SMITH - TX				
4	Mr. ROHRABACHER - CA				
5	Mr. BARTLETT - MD				
6	Mr. LUCAS - OK				
7	Mrs. BIGGERT - IL				
8	Mr. AKIN - MO				
9	Mr. NEUGEBAUER - TX				
10	Mr. McCAUL - TX				
11	Mr. BROUN - GA				
12	Mrs. ADAMS - FL				
13	Mr. QUAYLE - AZ				
14	Mr. FLEISCHMANN - TN				
15	Mr. RIGELL - VA				
16	Mr. PALAZZO - MS				
17	Mr. BROOKS - AL				
18	Mr. HARRIS - MD				
19	Mr. HULTGREN - IL				
20	Mr. CRAVAACK - MN				
21	Mr. BUCSHON - IN				
22	Mr. BENISHEK - MI				
23	Vacancy				
1	Ms. JOHNSON, *Ranking* - TX				
2	Mr. COSTELLO - IL				
3	Ms. WOOLSEY - CA				
4	Ms. LOFGREN - CA				
5	Mr. WU - OR				
6	Mr. MILLER - NC				
7	Mr. LIPINSKI - IL				
8	Ms. GIFFORDS - AZ				
9	Ms. EDWARDS - MD				
10	Ms. FUDGE - OH				
11	Mr. LUJÁN - NM				
12	Mr. TONKO - NY				
13	Mr. McNERNEY - CA				
14	Mr. SARBANES - MD				
15	Ms. SEWELL - AL				
16	Ms. WILSON - FL				
17	Mr. CLARKE - MI				
	TOTALS				

** Vice Chair

PREPARED STATEMENT OF REPRESENTATIVE FUDGE

Thank you, Mr. Chairman. I believe this is a straightforward amendment to Section 107, the Cybersecurity Workforce Assessment. I understand that what we are discussing is a matter of national security. We must ensure that our country's top talent is working to protect our information technology infrastructure, but we also must remember that our country has brilliant minds from coast to coast and everywhere in between.

Section 107 requires an assessment of the needs of the federal government, and an evaluation of the effectiveness of our programs in attracting and retaining professionals with the requisite level of expertise. As we do this, we need to make sure that we are including areas that have higher than average unemployment rates.

The IT and cybersecurity industry is growing dramatically as others remain in decline. I believe that my amendment will potentially give us the opportunity to address two problems simultaneously, and I urge my colleagues' support. Thank you.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 AMENDMENT NO. 032 ROLL CALL NO.____

Bill: H. R. 2096
SPONSOR: Mr. Lipinski

Agreed to in EnBloc
Amendments 6 of 6

Quorum –14 to vote –21 to report

MEMBER	AYE	NO	PRESENT	NOT VOTING
1 Mr. HALL, *Chair* - TX				
2 Mr. SENSENBRENNER – WI **				
3 Mr. SMITH - TX				
4 Mr. ROHRABACHER - CA				
5 Mr. BARTLETT - MD				
6 Mr. LUCAS - OK				
7 Mrs. BIGGERT - IL				
8 Mr. AKIN - MO				
9 Mr. NEUGEBAUER - TX				
10 Mr. McCAUL - TX				
11 Mr. BROUN - GA				
12 Mrs. ADAMS - FL				
13 Mr. QUAYLE - AZ				
14 Mr. FLEISCHMANN - TN				
15 Mr. RIGELL - VA				
16 Mr. PALAZZO - MS				
17 Mr. BROOKS - AL				
18 Mr. HARRIS - MD				
19 Mr. HULTGREN - IL				
20 Mr. CRAVAACK - MN				
21 Mr. BUCSHON - IN				
22 Mr. BENISHEK - MI				
23 Vacancy				
1 Ms. JOHNSON, *Ranking* - TX				
2 Mr. COSTELLO - IL				
3 Ms. WOOLSEY - CA				
4 Ms. LOFGREN - CA				
5 Mr. WU - OR				
6 Mr. MILLER - NC				
7 Mr. LIPINSKI - IL				
8 Ms. GIFFORDS - AZ				
9 Ms. EDWARDS - MD				
10 Ms. FUDGE - OH				
11 Mr. LUJÁN - NM				
12 Mr. TONKO - NY				
13 Mr. McNERNEY - CA				
14 Mr. SARBANES - MD				
15 Ms. SEWELL - AL 16 Ms. WILSON - FL 17 Mr. CLARKE - MI				
TOTALS				

** Vice Chair

PREPARED STATEMENT OF REPRESENTATIVE LIPINSKI

Thank you Mr. Chairman.

My amendment begins to address some of the cybersecurity issues specific to "cloud computing," by which I mean the practice of having software, data storage, or processing power hosted in an offsite data center which is accessed remotely via a network.

"The Cloud" is big business. Worldwide spending on cloud services in 2009 was estimated to be in excess of $54 billion, and it is expected to triple in size by 2013. The Administration has announced its intent to adopt cloud computing through its "Cloud First" policy, and some agencies –including GSA and USDA–have already begun migrating some IT systems to the cloud.

This is, in general, a good thing. The Federal government spends over $80 billion a year on IT systems. By moving some systems to the cloud it is projected we can save $5 billion, and by consolidating our 2000 data centers we can save billions more. Given our budget deficit, this is something we need to be doing.

The Cloud has other potential benefits too. It can avoid system duplication and potentially improve security. But rapid migration of federal IT systems to the cloud also raises questions: Where will data centers and IT jobs be located? Will our data be secure? Can we access it in an emergency?

I believe that cloud data centers should be located here in the US. We need the jobs, we need to make sure sensitive data is protected, and we need to make sure government data is under the protection of US law. I also want to make sure that individual agencies don't lock themselves into contracts that are proprietary or not interoperable with other clouds.

My amendment is intended to make sure that, as the Administration moves toward its "Cloud First" strategy, that it considers these issues.

Already, NIST has been working to develop a comprehensive strategy for interoperability standards, ensuring that information can be exchanged between cloud services. My amendment provides support for these activities, and it also requires NIST to consider the security and accessibility of information stored in the cloud.

By requiring NIST to develop a security framework that examines all possible weaknesses, including physical security and location, I believe that they will produce a strategy that gives the best chance of preventing cyber-theft before it can happen.

It is important for Congress to give cybersecurity in the cloud the attention it deserves, especially early-on in the development of our cloud strategy. I think my amendment appropriately emphasizes a few key areas of concern, without being overly prescriptive about how we should adopt cloud services.

I urge my colleagues to support this amendment and yield back the balance of my time.

Let me repeat for the record, this involves amendments 030, 032, 033, 042, 027, 003 and 032—wait a minute. Exclude 003. That is a Clarke amendment. We have some problems with that. And amendment 032. That is six.

The CLERK. That is five, Mr. Chairman.

Chairman HALL. Clerk, please repeat those, if you would, for the record.

The CLERK. I have 030, 032, 037, 042, 027. We crossed out 003. And then you said 032 again.

Chairman HALL. Alright. I am going to go out and come in again.

The CLERK. Okay.

Chairman HALL. 030, Luján; 032, Luján; 033, Luján; 042, Smith; 027, Fudge; 032, Lipinski. Now read back.

The CLERK. Amendment number 030, Mr. Luján; amendment number 032, Mr. Luján; amendment number 033, Mr. Luján; amendment number 042, Mr. Smith; amendment number 027, Ms. Fudge, amendment number 032, Mr. Lipinski.

[The amendments appears in the Appendix]

Mr. LUJÁN. Mr. Chairman, just some clarification. I just want to——

Chairman HALL. The Chair recognizes Mr. Luján.

Mr. LUJÁN. Thank you, Mr. Chairman.

I just want to make sure that with Mr. Lipinski's amendment number 032 and Luján's number 032 that there is not any confusion, that there is two separate amendments and that they will both be included.

Chairman HALL. I guess the answer is, that is correct. Is there further discussion?

Mr. LIPINSKI. Mr. Chairman?

Chairman HALL. Who seeks recognition?

Mr. LIPINSKI. Over here, Mr. Lipinski.

Chairman HALL. Mr. Lipinski, the Chair recognizes you for a quick five minutes.

Mr. LIPINSKI. It will be much shorter. I just wanted to clarify, are we precluding debate time on this or—because I know we are trying to—Mr. Bartlett is trying to move this more quickly, which I agree with, but are we limiting debate time or are we just saying they will be voted on together?

Chairman HALL. Yes, it is in the interest of time, but if you have a statement you want to make, you can submit it for the record, and any Member can submit it for the record. Does the gentleman yield back?

Mr. LIPINSKI. I yield back. I just wanted to clarify for everybody what we are doing here, if we are going to preclude any debate because I know procedurally we could strike the last word to speak but I know the intention here is to essentially ask everyone to not do that or—I just want to make this flow more smoothly here if we can so we all understand what we are doing.

Chairman HALL. I hope. And yes, that is the understanding.

Who seeks recognition?

Mr. CLARKE. Mr. Chairman, I do have an amendment at the desk.

Chairman HALL. Mr. Clarke. The clerk will report the amendment.

The CLERK. Amendment number 003, amendment to H.R. 2096, offered by Mr. Clarke of Michigan.

[The amendment appears in the Appendix]

Chairman HALL. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

The gentleman is recognized for five minutes to explain his amendment.

Mr. CLARKE. Thank you, Mr. Chair.

I am offering this amendment to clarify the need for more research and development to protect the digital identities, and that is to protect the American people from fraud and identify theft, and here is the reason why I ask you to consider this.

You know, personally, I am a guy that doesn't believe in borrowing money and using credit cards and consumer debt, and I don't buy anything online because I don't want to put my debit card and my money at risk like this. This is so important that we continue this type of research. It is already happening so we are not asking for anything new. This is actually going on right now, but this language will underscore the importance of continuing this type of research in digital identity to help protect Americans from fraud and theft when they want to buy something online, so it is going to help commerce, it is going to help our economy and maybe give assurances to people like me who use debit cards that they can go and buy things online without getting their identity stolen or their money stolen as well.

So I urge your support, and I do ask your consideration of this amendment. Again, there is no new money here. This program is going on right now. This language is just to underscore the need for the research and development that is going on right at this moment.

Chairman HALL. I want to thank you for the amendment. Do you yield back?

Mr. CLARKE. Mr. Chair, I do yield back my time.

Chairman HALL. Is there further discussion on the amendment?

Mr. MCCAUL. Mr. Chairman.

Chairman HALL. The Chair recognizes the gentleman from Texas.

Mr. MCCAUL. Thank you, and I want to thank the gentleman for his thoughtful amendment, and I agree that anybody who has ever been a victim of identity theft certainly understands, you know, the threat.

The bill already asks NIST to continue important research in this area. The implementation plan proposed, though, has not been, in my judgment, fully examined by this Committee and stakeholders before we move away from the R&D portion of what is happening at NIST.

So having had little time to gather feedback from the parties, I must withhold my support for this amendment today, and with that, I yield back.

Chairman HALL. The gentleman yields back.

I too am concerned about further broadening these activities at NIST take a big step toward implementation until we have heard from some of the stakeholders, as the gentleman from Texas has set out.

Is there further discussion on the amendment?

Mr. CLARKE. Yes, Mr. Chair. I would like to address it if I have time.

Chairman HALL. Who seeks recognition?

Mr. CLARKE. It is the maker of the amendment.

Chairman HALL. Mr. Clarke, you are recognized for five minutes.

Mr. CLARKE. Thank you again, Mr. Chair.

This is already being implemented right now.

Chairman HALL. I beg your pardon?

Mr. CLARKE. This research is already being implemented right now. This is in response to the other Members' question. This will just underscore the importance of the framework to make sure that these agencies continue to do this research.

Chairman HALL. Does the gentleman yield back?

Mr. CLARKE. Yes.

Chairman HALL. Is there further discussion on the amendment? Hearing no further discussion, the vote occurs on the amendment. All in favor, say aye.

Mr. CLARKE. Mr. Chair?

Chairman HALL. Those opposed, say no. The no's have it and the amendment is not agreed to.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 AMENDMENT NO. 003 ROLL CALL NO._____

Bill: H. R. 2096
SPONSOR: Mr.Clarke

Not agreed to by Voice Vote

Quorum –14 to vote –21 to report

MEMBER	AYE	NO	PRESENT	NOT VOTING
1 Mr. HALL, *Chair* - *TX*				
2 Mr. SENSENBRENNER – *WI* **				
3 Mr. SMITH - *TX*				
4 Mr. ROHRABACHER - *CA*				
5 Mr. BARTLETT - *MD*				
6 Mr. LUCAS - *OK*				
7 Mrs. BIGGERT - *IL*				
8 Mr. AKIN - *MO*				
9 Mr. NEUGEBAUER - *TX*				
10 Mr. McCAUL - *TX*				
11 Mr. BROUN - *GA*				
12 Mrs. ADAMS - *FL*				
13 Mr. QUAYLE - *AZ*				
14 Mr. FLEISCHMANN - *TN*				
15 Mr. RIGELL - *VA*				
16 Mr. PALAZZO - *MS*				
17 Mr. BROOKS - *AL*				
18 Mr. HARRIS - *MD*				
19 Mr. HULTGREN - *IL*				
20 Mr. CRAVAACK - *MN*				
21 Mr. BUCSHON - *IN*				
22 Mr. BENISHEK - *MI*				
23 Vacancy				
1 Ms. JOHNSON, *Ranking* - *TX*				
2 Mr. COSTELLO - *IL*				
3 Ms. WOOLSEY - *CA*				
4 Ms. LOFGREN - *CA*				
5 Mr. WU - *OR*				
6 Mr. MILLER - *NC*				
7 Mr. LIPINSKI - *IL*				
8 Ms. GIFFORDS - *AZ*				
9 Ms. EDWARDS - *MD*				
10 Ms. FUDGE - *OH*				
11 Mr. LUJÁN - *NM*				
12 Mr. TONKO - *NY*				
13 Mr. McNERNEY - *CA*				
14 Mr. SARBANES - *MD*				
15 Ms. SEWELL - *AL*				
16 Ms. WILSON - *FL*				
17 Mr. CLARKE - *MI*				
TOTALS				

** Vice Chair

Are there any other amendments?

Mr. LUJÁN. Mr. Chairman, I move to strike the last word.

Chairman HALL. The gentleman is recognized.

Mr. LUJÁN. I yield to Mr. Clarke.

Mr. CLARKE. Thank you, Mr. Luján.

I will choose not to ask for a recorded vote. Thank you.

Chairman HALL. Alright. Are there any other amendments?

Ms. JOHNSON. Mr. Chairman—oh, he just came in.

Chairman HALL. Mr. Wu, for what purpose does the gentleman seek recognition?

Mr. WU. Mr. Chairman, I have an amendment at the desk.

Chairman HALL. The next amendment is offered by Mr. Wu. It is amendment 020. Are you ready to proceed with your amendment?

Mr. WU. Yes, Mr. Chairman. I will give a very——

Chairman HALL. The clerk will report the amendment.

The CLERK. Amendment number 020, amendment to H.R. 2096, offered by Mr. Wu of Oregon.

[The amendment appears in the Appendix]

Chairman HALL. I ask unanimous consent to dispense with the reading. Without objection, it is so ordered.

The gentleman is recognized for five minutes to explain his amendment.

Mr. WU. Thank you, Mr. Chairman. I will offer a very truncated statement.

My amendment would give authority to the Director of NIST to convene representatives of the private sector and other relevant stakeholders, including consumer groups to collaborate on the development of consensus standards, guidelines, best practices and voluntary codes of conduct related to information technology security for use by certain private sector entities.

As the Committee knows, most of America's IT infrastructure is in the private sector and these security standards are incredibly important and NIST has been very good at convening stakeholders to develop consensus standards, and I believe this to be a very helpful amendment and urge adoption.

Chairman HALL. The gentleman yields back.

Actually, we have heard from industry groups that are very concerned about your amendment, Mr. Wu, that it might be moving a little too quickly, given that it is based on a green paper that was only released last month and has yet to close a comment period. I think we need some more time for companies and groups that would be affected by this legislation.

I yield the remainder of my five minutes to Mr. McCaul for his suggestions on this amendment.

Mr. MCCAUL. And thank you, Mr. Chairman.

Let me just say, Mr. Wu, conceptually, I think this is a great idea. I think NIST is probably the best vehicle to work with the private sector to establish voluntary guidelines and standards within the industry, and they have the expertise. I think the concern that has been highlighted to us from the technology companies is that the Department of Commerce has examined this, and there is a green paper that is out. What this amendment essentially would do, it would codify what is in the green paper and all they ask for is time between now and the white paper. They are receiving input

now from the private sector, and I think the technology companies would prefer that we wait until the white paper comes out when Department of Commerce and NIST has received this public comment.

My understanding is that this will take place in the month of August, well prior to this bill coming onto the floor, and so I would offer my sincere commitment to working with you because I do believe conceptually this is on the right track and what we need to do.

So with that, I would really like to follow up and work with you on this. I would hope you would withdraw it if you can with that commitment that I personally will commit to that, because I do think conceptually you are on the right track here. I just think it is premature until that white paper comes out.

Mr. WU. Will the gentleman yield?

Mr. MCCAUL. I would be happy to yield, yes.

Mr. WU. I thank the gentleman for his very helpful comments. This is not inconsistent at all with the gentleman's comments but I think that one of the reasons why private industry is more eager to work with NIST is because they are consensus standards that NIST develops and not regulatory requirements as some other agencies propound. I think that it is very helpful to await some further development, and I am very open to working with the gentleman, whether it is a second-order amendment today, which I take the gentleman to not be offering, or to work together as this legislation goes forward toward the House floor to develop the appropriate incorporation of green and white paper recommendations, and with that, I yield back to the gentleman.

Mr. MCCAUL. Thank you. Reclaiming my time. If I could just say, I agree with you that NIST is the best vehicle I think to work with the private sector as opposed to other agencies, and I think the private sector recognizes that as well on these consensus voluntary standards, and as with the Ranking Member's amendment, perhaps we can after the white paper comes out—I just don't want to codify what is in a green paper. I would rather codify what is in a white paper, if that makes sense. And then we can go back, and if there is going to be a Manager's Amendment, which is looks like there would be on the floor, we can incorporate these very good ideas at that time.

Thank you. I yield back.

Chairman HALL. The gentleman yields back.

Does anyone else request time? Mr. Wu, I recognize you. I think you have about three minutes left on your five, but I will give you five more.

Mr. WU. Mr. Chairman, I have a separate amendment. I have an amendment at the desk.

Chairman HALL. Might I inquire, did I understand you to——

Mr. WU. My apologies. On the prior amendment, I would like permission to withdraw the amendment.

Chairman HALL. Without objection, it is withdrawn. I thank the gentleman.

Do you have a second amendment?

Mr. WU. Yes, Mr. Chairman.

Chairman HALL. Do you have an amendment at the desk?

Mr. WU. Yes, Mr. Chairman.

Chairman HALL. We have an amendment offered by the gentleman from Oregon. Are you ready to proceed with your amendment?

Mr. WU. Yes, Mr. Chairman, I am.

Chairman HALL. Alright, the clerk will report the amendment.

The CLERK. Amendment number 019, amendment to H.R. 2096, offered by Mr. Wu of Oregon.

[The amendment appears in the Appendix]

Chairman HALL. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

The gentleman is recognized for five minutes to explain his amendment.

Mr. WU. Thank you very much, Mr. Chairman.

My amendment is intended to highlight the unique and important role that community colleges can, should and are playing in cybersecurity education and the training of cybersecurity professionals. In addition to serving on this Committee, I serve as a co-chair of the Congressional Community College Caucus. Community colleges are often times best suited to educate and train and retrain students in order to meet the employment needs of local businesses. Moreover, community colleges play a crucial role in educating our science and technology workforce. The American Association of Community Colleges estimates that 44 percent of students who receive baccalaureates or master's degrees in STEM fields attended a community college at some point in their careers.

My amendment is simple. It requires the Director of NIST to carry out an assessment of community colleges and cybersecurity education, including a description of the current role of communities in cybersecurity education and identification of best practices and recommendations on steps the Federal Government can take to improve or bolster the role of community colleges.

As we are all aware, NIST has been charged with coordinating and overseeing the interagency National Initiative on Cybersecurity Education, or NICE, which is a broad initiative focused on several critical aspects of cybersecurity education and the development of a skilled cybersecurity workforce. Although this initiative is not clearly spelled out in the underlying bill, it is my intent that the Director of NIST be in charge of this assessment in his capacity as the coordinator and overseer of NICE. It is my expectation that the Director will coordinate and oversee the other agencies that are part of the initiative in the development of this assessment and not carry out this assessment on his own.

I think there is value to having the participation of all the agencies involved in cybersecurity education in the assessment, and NICE seems like an appropriate place to ensure that this will happen.

I am aware that the workforce assessment under section 107 includes an examination of the capacity of institutions of higher education, including community colleges to provide cybersecurity professionals with the skills sought by the Federal Government and the private sector. This is certainly important, and I support it. However, I note that in section 107, community colleges are but one small mention in a small piece of a much larger workforce assessment. For all intents and purposes, in section 107 community colleges are no more than an afterthought. I believe that commu-

nity colleges deserve a much more though and comprehensive look and that it is important that we pull them out and give them the respect they deserve. They have been frequently underserved and not at the table in Congressional consideration. There is no doubt that community colleges have an important role to play in training future cybersecurity professionals and indeed in taking existing computer professionals and retraining them for cybersecurity roles or tooling them up further.

Not only are they in a position to train students just entering the workforce but they can also play a unique role in retraining. We often hear about the need for more skilled cybersecurity professionals and at the same time in this tough economy, too many people are out of work and looking for jobs.

My amendment is intended to fill a gap that was left between the bill from the last Congress and the bill introduced in this Congress. I believe it to be a good amendment, one that is good for the workforce and good to complete the education array from high school through graduate school, and I recommend an aye vote on this amendment.

Chairman HALL. Does the gentleman yield back?

Mr. WU. Yes, Mr. Chairman.

Chairman HALL. I thank the Member for his amendment. Is there further discussion on the amendment?

Mr. MCCAUL. Mr. Chairman.

Chairman HALL. Who seeks recognition?

Mr. MCCAUL. Mr. McCaul.

Chairman HALL. Mr. McCaul, I recognize you for five minutes.

Mr. MCCAUL. Thank you, and let me say first, I agree with the gentleman that community colleges play a vital role in the education and development of a cybersecurity workforce. I think our concern with the amendment is that it is to be carried out by NIST, and I think there is a genuine debate over whether that is something NIST should be in the business of doing.

In the assessment section of this bill, it says that the President is to address cybersecurity workforce needs in a report to Congress, and it included language, and I will just read the quote directly from the bill, "an examination of the current and future capacity of the United States institutions of higher education, including community colleges."—that is in this bill—"to provide cybersecurity professionals with those skills sought by the Federal Government and the private sector."

So I believe that the bill again points out this determination should be made at the Presidential level, not at NIST, and I was wondering if the Ranking Member would be willing to withdraw his amendment and work with us on some report language to the workforce assessment section of the bill on this topic, and I would be happy to yield to the gentleman.

Mr. WU. I thank the gentleman.

I would be eager to work with the gentleman, either on report language or perhaps statutory language to be included in this legislation as we move forward with this legislation to the floor, and the reason why I want to keep open the possibility of statutory language is that cybersecurity is, as the gentleman knows, currently scattered in a number of different places. Education functions are also scattered in a number of different agencies and technical or cy-

bersecurity education is no exception, and I believe that the ARPA–E, or America COMPETES legislation, I should say, that we passed has tasked a number of different agencies with education functions and that the Manufacturing Education Program or MEP has specifically tasked NIST with some education functions so I would like the gentleman to remain open to having some education components in NIST because as we work together on this, we may find that there are pretty well related education components in NIST and there may be more leeway in this Presidential directive, and I find it very nice that the Majority is interested in heeding this particular Presidential directive, and I yield back to the gentleman.

Mr. MCCAUL. And I thank you and I look forward to working with you on this.

Chairman HALL. Does the gentleman withdraw 019——

Mr. WU. I thank the gentleman.

Chairman HALL. —agreement for report language?

Mr. WU. I thank both gentlemen from Texas, and I ask unanimous consent to withdraw my amendment.

Chairman HALL. The gentleman withdraws.

Is there further discussion? Hearing no further discussion, the vote will not occur on this amendment. We will go to the next amendment.

Any other amendments?

Mr. TONKO. Yes, Mr. Chair, I have an amendment at the desk.

Chairman HALL. The next amendment is offered by the gentleman from New York, Mr. Tonko. Are you ready to proceed with your amendment?

Mr. TONKO. I am, Mr. Chair.

Chairman HALL. The clerk will report the amendment.

The CLERK. Amendment number 001, amendment to H.R. 2096, offered by Mr. Tonko of New York.

[The amendment appears in the Appendix]

Chairman HALL. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

The gentleman is recognized for five minutes to explain his amendment.

Mr. TONKO. I thank you, Mr. Chairman.

My amendment today is simple and straightforward and addresses one of the biggest concerns repeatedly heard from our Republican colleagues. On any given day in Congress, you can go to the House floor and hear Members of Congress speak about how unfunded mandates and government regulation are hurting the economy. While I don't agree that regulation hurts the economy, I do, however, believe that if government is going to set policies on businesses or agencies, we should give them the financial tools by which to meet those policies.

My amendment does just that. It prevents unfunded mandates from taking effect if Congress does not also provide the funding to implement them. My amendment states that the activities mandated in section 108 significant to the cybersecurity university-industry taskforce are not required to be carried out for any fiscal year unless the amount appropriated to the Office of Science and Technology Policy, OSTP, is equal to or greater than the amount appropriated to the OSTP in fiscal year 2011's Continuing Resolution.

The amendment also states that the activities mandated in section 110, the identify management framework, section 202, the international technical standards, and section 203, the cybersecurity awareness and education program, are not required to be carried out for any fiscal year unless the amount appropriated to the National Institute of Standards and Technology, NIST, is equal to or greater than the amount appropriated to NIST in the fiscal year 2011 Continuing Resolution.

NIST has indicated that under the proposed fiscal year 2012 funding level, it would be unable to carry out any of the additional cybersecurity-related activities with which it has been charged over the last couple of years. The Administration has made significant progress in meeting the near-term actions outlined in Cyberspace Policy Review and NIST has a prominent role in fulfilling those objectives. For instance, under lower funding levels, NIST will no longer be able to coordinate the National Cybersecurity Education Initiative, or NICE, implement the National Strategy for Trusted Identities in Cyberspace or carry out a number of its cloud computing security activities. Again, under this amendment, if the NIST or the OSTP budgets dip below the level in the fiscal year 2011 Continuing Resolution, both would be relieved of implementing the additional mandates in this legislation.

Our cybersecurity is a serious concern, and as Members of this Committee, we should understand the importance of authorizing funding to go along with the policies we mandate to protect us from these types of attacks. The growing access to the Internet across the globe has proven to bring people together but is also increasing the opportunities unfriendly nations and groups have that wish to launch cyber attacks against us.

One of the most recent attacks was reported by Google last month. The company reported that Chinese hackers had broken into the gmail accounts of U.S. politicians. The latest reports indicate that the account of at least one Cabinet-level official was compromised. Sadly, these attacks will continue regardless of what we do in this Committee today. However, what we can control today is whether or not we are going to provide all the necessary tools to the agencies that are charged with protecting us from future attacks.

As Members of this Committee, if we are truly committed to our national security and want to prevent additional unfunded mandates passed by Congress, then we should all vote for this amendment, and I urge all my colleagues to do just that and support this amendment.

Thank you, Mr. Chair. With that, I yield back.

Chairman HALL. I thank the Member for his amendment. He yields back.

Is there further discussion on the amendment?

Mr. MCCAUL. Mr. Chairman.

Chairman HALL. The gentleman from Texas.

Mr. MCCAUL. I understand the gentleman's point.

Chairman HALL. I yield five minutes to the gentleman from Texas.

Mr. MCCAUL. Thank you.

I think it is important to point out that these activities in this bill we authorized for NIST are already being carried out by NIST

and have for some time, within the allocated budget. We are merely utilizing its authority to give some direction to these activities. I think that certainly it is within Congress's role to influence agency actions. This amendment would say that we couldn't do that unless we appropriate more money each year, and I think it is—we have to be realistic within the confines of our current budget situation and the federal deficit that we keep in line with that, and on a practical note, I think this type of amendment would jeopardize this bill's passage on the floor, but I certainly understand the gentleman's points, and with that I yield back.

Chairman HALL. The gentleman yields back.

Is there further discussion?

Ms. EDWARDS. Mr. Chairman.

Chairman HALL. Who seeks recognition? The Chair recognizes Ms. Edwards for five minutes.

Ms. EDWARDS. Thank you, Mr. Chairman, and I will be brief and thank the gentleman.

I really support the efforts by the gentleman from New York. We are constantly asking our federal agencies and those who work with these agencies to do more with less, and that is particularly true when it comes to areas of science and technology under this Committee's jurisdiction, and my concern is that when we do that and then they fail to meet goals and they fail to achieve objectives, we bring them before this Committee and other Committees in the Congress and we chastise them for not meeting the goals and the objectives when we have taken away the resources with which they need to do that. I think that is an unreasonable expectation to say that we want the agency to continue to fulfill its responsibilities, add additional responsibilities and then not—and then flatline their funding and not give them the funding that they need, and I think that the gentleman's amendment that is at the desk in front of us simply seeks to give us a little bit of discipline in terms of what we expect of agencies, and either we want them to do the work and achieve the goals that we set out with appropriate resources or we shouldn't ask them to do the work, and I am particularly sensitive to that.

NIST is headquartered in my district. I am out there all the time. I see the work that they do and appreciate their professionalism, but we have to stop asking our agencies to do more work with fewer resources, and with that I yield.

Chairman HALL. The gentlelady yields back her time.

Is there further discussion on the amendment? The Chair hears none. Hearing no further discussion, the vote will occur on the amendment. All in favor, say aye. All opposed, say no. In the Chair's opinion, the no's have it.

Mr. TONKO. Mr. Chairman, I ask for a recorded vote, please.

Chairman HALL. Recorded vote is requested. The clerk will call the roll.

The CLERK. Chairman Hall?

Chairman HALL. No.

The CLERK. Chairman Hall votes no.

Mr. Sensenbrenner?

Mr. SENSENBRENNER. No.

The CLERK. Mr. Sensenbrenner votes no.

Mr. Smith?

Mr. SMITH. No.
The CLERK. Mr. Smith votes no.
Mr. Rohrabacher?
Mr. ROHRABACHER. No.
The CLERK. Mr. Rohrabacher votes no.
Mr. Bartlett?
Mr. BARTLETT. No.
The CLERK. Mr. Bartlett votes no.
Mr. Lucas?
[No response.]
The CLERK. Mrs. Biggert?
Mrs. BIGGERT. No.
The CLERK. Mrs. Biggert votes no.
Mr. Akin?
[No response.]
The CLERK. Mr. Neugebauer?
[No response.]
The CLERK. Mr. McCaul?
Mr. MCCAUL. No.
The CLERK. Mr. McCaul votes no.
Mr. Broun?
Mr. BROUN. No.
The CLERK. Mr. Broun votes no.
Mrs. Adams?
Mrs. ADAMS. No.
The CLERK. Mrs. Adams votes no.
Mr. Quayle?
[No response.]
The CLERK. Mr. Fleischmann?
Mr. FLEISCHMANN. No.
The CLERK. Mr. Fleischmann votes no.
Mr. Rigell?
Mr. RIGELL. No.
The CLERK. Mr. Rigell votes no.
Mr. Palazzo?
Mr. PALAZZO. No.
The CLERK. Mr. Palazzo votes no.
Mr. Brooks?
Mr. BROOKS. No.
The CLERK. Mr. Brooks votes no.
Mr. Harris?
Mr. HARRIS. No.
The CLERK. Mr. Harris votes no.
Mr. Hultgren?
Mr. HULTGREN. No.
The CLERK. Mr. Hultgren votes no.
Mr. Cravaack?
Mr. CRAVAACK. No.
The CLERK. Mr. Cravaack votes no.
Mr. Bucshon?
[No response.]
The CLERK. Mr. Benishek?
Mr. BENISHEK. No.
The CLERK. Mr. Benishek votes no.
Ms. Johnson?

Ms. JOHNSON. Aye.
The CLERK. Ms. Johnson votes aye.
Mr. Costello?
Mr. COSTELLO. Aye.
The CLERK. Mr. Costello votes aye.
Ms. Woolsey?
[No response.]
The CLERK. Ms. Lofgren?
Ms. LOFGREN. Aye.
The CLERK. Ms. Lofgren votes aye.
Mr. Wu?
Mr. WU. Aye.
The CLERK. Mr. Wu votes aye.
Mr. Miller?
[No response.]
The CLERK. Mr. Lipinski?
Mr. LIPINSKI. Aye.
The CLERK. Mr. Lipinski votes aye.
Ms. Giffords?
[No response.]
The CLERK. Ms. Edwards?
Ms. EDWARDS. Aye.
The CLERK. Ms. Edwards votes aye.
Ms. Fudge?
Ms. FUDGE. Aye.
The CLERK. Ms. Fudge votes aye.
Mr. Luján?
Mr. LUJÁN. Aye.
The CLERK. Mr. Luján votes aye.
Mr. Tonko?
Mr. TONKO. Aye.
The CLERK. Mr. Tonko votes aye.
Mr. McNerney?
Mr. MCNERNEY. Aye.
The CLERK. Mr. McNerney votes aye.
Mr. Sarbanes?
[No response.]
The CLERK. Ms. Sewell?
Ms. SEWELL. Aye.
The CLERK. Ms. Sewell votes aye.
Ms. Wilson?
Ms. WILSON. Aye.
The CLERK. Ms. Wilson votes aye.
Mr. Clarke?
Mr. CLARKE. Aye.
The CLERK. Mr. Clarke votes aye.

Chairman HALL. Are there other Members who wish to vote? Other Members who wish to vote?

Is the clerk ready to report the vote?

The CLERK. Mr. Chairman, 13 Members vote aye and 17 Members vote no.

Chairman HALL. On this vote, there were 13 ayes and 17 no's. The amendment is not agreed to.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 112th

DATE: July 21, 2011 AMENDMENT NO. 001 ROLL CALL NO. 1

Bill: H. R. 2096
SPONSOR: Mr. Tonko

Not agreed to by a vote of 13 yeas and 17 nays

Quorum –14 to vote –21 to report

MEMBER	AYE	NO	PRESENT	NOT VOTING
1 Mr. HALL, *Chair* - TX		X		
2 Mr. SENSENBRENNER – WI **		X		
3 Mr. SMITH - TX		X		
4 Mr. ROHRABACHER - CA		X		
5 Mr. BARTLETT - MD		X		
6 Mr. LUCAS - OK				
7 Mrs. BIGGERT - IL		X		
8 Mr. AKIN - MO				
9 Mr. NEUGEBAUER - TX				
10 Mr. McCAUL - TX		X		
11 Mr. BROUN - GA		X		
12 Mrs. ADAMS - FL		X		
13 Mr. QUAYLE - AZ				
14 Mr. FLEISCHMANN - TN		X		
15 Mr. RIGELL - VA		X		
16 Mr. PALAZZO - MS		X		
17 Mr. BROOKS - AL		X		
18 Mr. HARRIS - MD		X		
19 Mr. HULTGREN - IL		X		
20 Mr. CRAVAACK - MN		X		
21 Mr. BUCSHON - IN				
22 Mr. BENISHEK - MI		X		
23 Vacancy				
1 Ms. JOHNSON, *Ranking* - TX	X			
2 Mr. COSTELLO - IL	X			
3 Ms. WOOLSEY - CA				
4 Ms. LOFGREN - CA	X			
5 Mr. WU - OR	X			
6 Mr. MILLER - NC				
7 Mr. LIPINSKI - IL	X			
8 Ms. GIFFORDS - AZ				
9 Ms. EDWARDS - MD	X			
10 Ms. FUDGE - OH	X			
11 Mr. LUJÁN - NM	X			
12 Mr. TONKO - NY	X			
13 Mr. McNERNEY - CA	X			
14 Mr. SARBANES - MD				
15 Ms. SEWELL - AL	X			
16 Ms. WILSON - FL	X			
17 Mr. CLARKE - MI	X			
TOTALS	13	17		

** Vice Chair

Are there any other amendments? Hearing none, the question is on the bill, H.R. 2096, the Cybersecurity Enhancement Act of 2011 as amended. All those in favor will say aye. All those opposed, say no. In the opinion of the Chair, the ayes have it. The ayes have it. The bill is passed.

Alright. Now that we have passed the bill and we have agreed to it, I want to recognize the gentleman from Texas, Mr. McCaul, to offer a motion.

Mr. MCCAUL. And thank you, Mr. Chairman.

Before I offer the motion, I just want to again thank you and the Ranking Member and Mr. Lipinski for all of your hard work on this issue. It is refreshing at a time when we have so many issues that divide us, this is one of those issues that I think brings us together, and so with that, I move that the Committee favorably report H.R. 2096 as amended to the House with the recommendation that the bill do pass.

Furthermore, I move that staff be instructed to prepare the legislative report and make necessary technical and conforming changes and that the Chairman take all necessary steps to bring the bill before the House for consideration.

Ms. WOOLSEY. Mr. Chairman?

Chairman HALL. Who seeks recognition?

Ms. WOOLSEY. Me, down here, Lynn Woolsey. I would like to ask——

Chairman HALL. Ms. Woolsey, I am in the process of calling the vote right now. I will recognize you in just a moment.

Ms. WOOLSEY. Okay. I am sorry, sir.

Chairman HALL. The question is on the motion to report the bill. Those in favor will say aye. Those opposed, say no. The ayes have it and the resolution is reported.

Without objection, the motion to reconsider is laid upon the table. Members have two subsequent calendar days in which to submit supplemental minority or additional views on the measure. I move pursuant to clause 1 of rule 22 of the Rules of the House of Representatives that the Committee authorizes the Chairman to offer such motions as may be necessary in the House to adopt and pass H.R. 2096, the Cybersecurity Enhancement Act of 2011 as amended. Without objection, it is so ordered.

The Chair now recognizes Ms. Woolsey.

Ms. WOOLSEY. Thank you, Mr. Chairman. I would like to ask unanimous consent to vote for Mr. Tonko's amendment, and I would have voted yes. I don't think it changes the total at all.

Mr. BROUN. Mr. Chairman.

Ms. WOOLSEY. I was on my way over here.

Chairman HALL. Who seeks recognition?

Mr. BROUN. I object.

Chairman HALL. There is an objection.

Mr. LUJÁN. Mr. Chairman.

Chairman HALL. Mr. Luján, you are recognized for five minutes.

Mr. LUJÁN. Mr. Chairman, at the time that votes said that they were going to be rolled, we were told Members would be notified, and there was no notification for Members to vote, and now there is an objection when a Member showed up to ask UC to be included here. I think that we are just asking for some fairness for those

Members that did make it back and those Members that did want to vote that were told we would be notified before we would vote.

Mr. BROUN. Mr. Chairman.

Chairman HALL. The Chair recognizes Mr. Broun.

Mr. BROUN. Mr. Chairman, I have been convinced by my dear friend Mr. Luján and I will withdraw my objection.

Chairman HALL. The objection is withdrawn. Good job, Mr. Luján.

Ms. WOOLSEY. Yes, thanks, Mr. Luján.

Mr. NEUGEBAUER. Mr. Chairman.

Chairman HALL. Who seeks recognition?

Mr. NEUGEBAUER. Mr. Chairman, I guess I would fall in that category as well as I thought when we did the rolled votes that we were going to have some notification, and there is probably five or six police cars behind me that will be here any minute but we sped over here quickly. So I need to, you know, get out of here pretty quick before they get here, but I would like to be recorded.

Chairman HALL. We will let the record reflect that you would have voted——

Mr. NEUGEBAUER. Voted no. That is correct.

Chairman HALL. And we'll do your bond if they show up.

Mr. Lucas is recognized.

Mr. LUCAS. Mr. Chairman, I too was on the way and would like to be noted as a no vote.

Chairman HALL. I am going with you guys next time. Is there objection? The Chair hears none. Mr. Lucas will be voted no. Mr. Bucshon asked to be recorded as supported on the bill and no to the amendment.

Alright. I think the gentlelady from Texas wants to be heard.

Ms. JOHNSON. Thank you.

Chairman HALL. Mr. Quayle asked for a no vote on the amendment. Is there objection? Did we clear Mr. Bucshon? He asked for a no vote. Is there objection? The Chair hears none. Who else?

Now, the Chair recognizes the Ranking Member.

Ms. JOHNSON. Thank you, Mr. Chairman. I simply want to apologize for allowing my thoughts to become spoken words when I said we looked like a bunch of fools. I really meant it, but I don't—I usually don't do things like that in the midst of a full Committee, and I don't want to imply that I think this Committee is a bunch of fools. I think we are one of the most respected Committees for dealing with very intellectual material, and so I apologize for using that phrase.

What I was concerned about is the inflexibility of just making a simple correction. It is not common for this Committee in my years of being here to act so quickly in that way. However, knowing the times, and I respect you so much, I just want to apologize for allowing those thoughts to become spoken words. Thank you.

Chairman HALL. The gentlelady yields back to us, I suppose? The gentlelady yields back.

Alright. This concludes our full Committee markup.

[Whereupon, at 11:34 a.m., the Committee was adjourned.]

Appendix I:

H.R. 2096, Section-by-Section Analysis, Amendments, Amendment Roster

I

112TH CONGRESS
1ST SESSION

H. R. 2096

To advance cybersecurity research, development, and technical standards, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 2, 2011

Mr. MCCAUL (for himself and Mr. LIPINSKI) introduced the following bill; which was referred to the Committee on Science, Space, and Technology

---

A BILL

To advance cybersecurity research, development, and technical standards, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity Enhancement Act of 2011".

TITLE I—RESEARCH AND DEVELOPMENT

SEC. 101. DEFINITIONS.

In this title:

(1) NATIONAL COORDINATION OFFICE.—The term National Coordination Office means the National Coordination Office for the Networking and Information Technology Research and Development program.

(2) PROGRAM.—The term Program means the Networking and Information Technology Research and Development program which has been established under section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511).

SEC. 102. FINDINGS.

Section 2 of the Cyber Security Research and Development Act (15 U.S.C. 7401) is amended—

(1) by amending paragraph (1) to read as follows:

"(1) Advancements in information and communications technology have resulted in a globally interconnected network of government, commercial, scientific, and education infrastructures, including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services.";

(2) in paragraph (2), by striking "Exponential increases in interconnectivity have facilitated enhanced communications, economic growth," and inserting "These advancements have significantly contributed to the growth of the United States economy";

(3) by amending paragraph (3) to read as follows:

"(3) The Cyberspace Policy Review published by the President in May, 2009, concluded that our information technology and communications infrastructure is vulnerable and has 'suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information'."; and

(4) by amending paragraph (6) to read as follows:

"(6) While African-Americans, Hispanics, and Native Americans constitute 33 percent of the college-age population, members of these minorities comprise less than 20 percent of bachelor degree recipients in the field of computer sciences.".

SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DEVELOPMENT PLAN.

(a) IN GENERAL.—Not later than 12 months after the date of enactment of this Act, the agencies identified in subsection 101(a)(3)(B)(i) through (x) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)(i) through (x)) or designated under section 101(a)(3)(B)(xi) of such Act, working through the National Science and Technology Council and with the assistance of the National Coordination Office, shall transmit to Congress a strategic plan based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking systems. Once every 3 years after the initial strategic plan is transmitted to Congress under this section, such agencies shall prepare and transmit to Congress an update of such plan.

(b) CONTENTS OF PLAN.—The strategic plan required under subsection (a) shall—

(1) specify and prioritize near-term, mid-term and long-term research objectives, including objectives associated with the research areas identified in section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) and how the near-term objectives complement research and

development areas in which the private sector is actively engaged;

(2) describe how the Program will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure;

(3) describe how the Program will foster the transfer of research and development results into new cybersecurity technologies and applications for the benefit of society and the national interest, including through the dissemination of best practices and other outreach activities;

(4) describe how the Program will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems;

(5) describe how the Program will facilitate access by academic researchers to the infrastructure described in paragraph (4), as well as to relevant data, including event data; and

(6) describe how the Program will engage females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities

Act (42 U.S.C. 1885a or 1885b) to foster a more diverse workforce in this area.

(c) DEVELOPMENT OF ROADMAP.—The agencies described in subsection (a) shall develop and annually update an implementation roadmap for the strategic plan required in this section. Such roadmap shall—

(1) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated;

(2) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

(3) estimate the funding required for each major research objective of the strategic plan for the following 3 fiscal years.

(d) RECOMMENDATIONS.—In developing and updating the strategic plan under subsection (a), the agencies involved shall solicit recommendations and advice from—

(1) the advisory committee established under section 101(b)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)(1)); and

(2) a wide range of stakeholders, including industry, academia, including representatives of minority serving institutions and community colleges, and other relevant organizations and institutions.

(e) APPENDING TO REPORT.—The implementation roadmap required under subsection (c), and its annual updates, shall be appended to the report required under section 101(a)(2)(D) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)(D)).

SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSECURITY.

Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) by inserting "and usability" after "to the structure";

(2) in subparagraph (H), by striking "and" after the semicolon;

(3) in subparagraph (I), by striking the period at the end and inserting "; and"; and

(4) by adding at the end the following new subparagraph:

"(J) social and behavioral factors, including human-computer interactions, usability, user motivations, and organizational cultures.".

SEC. 105. NATIONAL SCIENCE FOUNDATION CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY RESEARCH AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (A) by inserting "identity management," after "cryptography,"; and

(2) in subparagraph (I), by inserting ", crimes against children, and organized crime" after "intellectual property".

(b) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—Section 4(a)(3) of such Act (15 U.S.C. 7403(a)(3)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $90,000,000 for fiscal year 2012;

"(B) $90,000,000 for fiscal year 2013; and

"(C) $90,000,000 for fiscal year 2014.".

(c) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—Section 4(b) of such Act (15 U.S.C. 7403(b)) is amended—

(1) in paragraph (4)—

(A) in subparagraph (C), by striking "and" after the semicolon;

(B) in subparagraph (D), by striking the period and inserting "; and"; and

(C) by adding at the end the following new subparagraph:

"(E) how the center will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions."; and

(2) in paragraph (7) by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $4,500,000 for fiscal year 2012;

"(B) $4,500,000 for fiscal year 2013; and

"(C) $4,500,000 for fiscal year 2014.".

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of such Act (15 U.S.C. 7404(a)(6)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $19,000,000 for fiscal year 2012;

"(B) $19,000,000 for fiscal year 2013; and

"(C) $19,000,000 for fiscal year 2014.".

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of such Act (15 U.S.C. 7404(b)(2)) is amended by striking subparagraphs (A)

through (E) and inserting the following new subparagraphs:

"(A) $2,500,000 for fiscal year 2012;

"(B) $2,500,000 for fiscal year 2013; and

"(C) $2,500,000 for fiscal year 2014.".

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY.—Section 5(c)(7) of such Act (15 U.S.C. 7404(c)(7)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

"(A) $24,000,000 for fiscal year 2012;

"(B) $24,000,000 for fiscal year 2013; and

"(C) $24,000,000 for fiscal year 2014.".

(g) CYBER SECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—Section 5(e) of such Act (15 U.S.C. 7404(e)) is repealed.

SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation shall continue a Scholarship for Service program under section 5(a) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)) to recruit and train the next generation of Federal cybersecurity professionals and to increase the capacity of the higher education system to produce an information technology

workforce with the skills necessary to enhance the security of the Nation's communications and information infrastructure.

(b) CHARACTERISTICS OF PROGRAM.—The program under this section shall—

(1) provide, through qualified institutions of higher education, scholarships that provide tuition, fees, and a competitive stipend for up to 2 years to students pursing a bachelor's or master's degree and up to 3 years to students pursuing a doctoral degree in a cybersecurity field;

(2) provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal information technology workforce; and

(3) increase the capacity of institutions of higher education throughout all regions of the United States to produce highly qualified cybersecurity professionals, through the award of competitive, merit-reviewed grants that support such activities as—

(A) faculty professional development, including technical, hands-on experiences in the private sector or government, workshops, seminars, conferences, and other professional devel-

opment opportunities that will result in improved instructional capabilities;

(B) institutional partnerships, including minority serving institutions and community colleges; and

(C) development of cybersecurity-related courses and curricula.

(c) SCHOLARSHIP REQUIREMENTS.—

(1) ELIGIBILITY.—Scholarships under this section shall be available only to students who—

(A) are citizens or permanent residents of the United States;

(B) are full-time students in an eligible degree program, as determined by the Director, that is focused on computer security or information assurance at an awardee institution; and

(C) accept the terms of a scholarship pursuant to this section.

(2) SELECTION.—Individuals shall be selected to receive scholarships primarily on the basis of academic merit, with consideration given to financial need, to the goal of promoting the participation of individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act

(42 U.S.C. 1885a or 1885b), and to veterans. For purposes of this paragraph, the term "veteran" means a person who—

(A) served on active duty (other than active duty for training) in the Armed Forces of the United States for a period of more than 180 consecutive days, and who was discharged or released therefrom under conditions other than dishonorable; or

(B) served on active duty (other than active duty for training) in the Armed Forces of the United States and was discharged or released from such service for a service-connected disability before serving 180 consecutive days.

For purposes of subparagraph (B), the term "service-connected" has the meaning given such term under section 101 of title 38, United States Code.

(3) SERVICE OBLIGATION.—If an individual receives a scholarship under this section, as a condition of receiving such scholarship, the individual upon completion of their degree must serve as a cybersecurity professional within the Federal workforce for a period of time as provided in paragraph (5). If a scholarship recipient is not offered employment by a Federal agency or a federally funded research

and development center, the service requirement can be satisfied at the Director's discretion by—

(A) serving as a cybersecurity professional in a State, local, or tribal government agency; or

(B) teaching cybersecurity courses at an institution of higher education.

(4) CONDITIONS OF SUPPORT.—As a condition of acceptance of a scholarship under this section, a recipient shall agree to provide the awardee institution with annual verifiable documentation of employment and up-to-date contact information.

(5) LENGTH OF SERVICE.—The length of service required in exchange for a scholarship under this subsection shall be 1 year more than the number of years for which the scholarship was received.

(d) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) GENERAL RULE.—If an individual who has received a scholarship under this section—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section; or

(E) fails to fulfill the service obligation of the individual under this section,

such individual shall be liable to the United States as provided in paragraph (3).

(2) MONITORING COMPLIANCE.—As a condition of participating in the program, a qualified institution of higher education receiving a grant under this section shall—

(A) enter into an agreement with the Director of the National Science Foundation to monitor the compliance of scholarship recipients with respect to their service obligation; and

(B) provide to the Director, on an annual basis, post-award employment information required under subsection (c)(4) for scholarship recipients through the completion of their service obligation.

(3) AMOUNT OF REPAYMENT.—

(A) LESS THAN ONE YEAR OF SERVICE.—If a circumstance described in paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(B) MORE THAN ONE YEAR OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(C) REPAYMENTS.—A loan described in subparagraph (A) or (B) shall be treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher Edu-

cation Act of 1965 (20 U.S.C. 1087a and following), and shall be subject to repayment, together with interest thereon accruing from the date of the scholarship award, in accordance with terms and conditions specified by the Director (in consultation with the Secretary of Education) in regulations promulgated to carry out this paragraph.

(4) COLLECTION OF REPAYMENT.—

(A) IN GENERAL.—In the event that a scholarship recipient is required to repay the scholarship under this subsection, the institution providing the scholarship shall—

(i) be responsible for determining the repayment amounts and for notifying the recipient and the Director of the amount owed; and

(ii) collect such repayment amount within a period of time as determined under the agreement described in paragraph (2), or the repayment amount shall be treated as a loan in accordance with paragraph (3)(C).

(B) RETURNED TO TREASURY.—Except as provided in subparagraph (C) of this para-

graph, any such repayment shall be returned to the Treasury of the United States.

(C) RETAIN PERCENTAGE.—An institution of higher education may retain a percentage of any repayment the institution collects under this paragraph to defray administrative costs associated with the collection. The Director shall establish a single, fixed percentage that will apply to all eligible entities.

(5) EXCEPTIONS.—The Director may provide for the partial or total waiver or suspension of any service or payment obligation by an individual under this section whenever compliance by the individual with the obligation is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(e) HIRING AUTHORITY.—For purposes of any law or regulation governing the appointment of individuals in the Federal civil service, upon successful completion of their degree, students receiving a scholarship under this section shall be hired under the authority provided for in section 213.3102(r) of title 5, Code of Federal Regulations, and be exempted from competitive service. Upon fulfillment of the service term, such individuals shall be con-

verted to a competitive service position without competition if the individual meets the requirements for that position.

SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.

Not later than 180 days after the date of enactment of this Act the President shall transmit to the Congress a report addressing the cybersecurity workforce needs of the Federal Government. The report shall include—

(1) an examination of the current state of and the projected needs of the Federal cybersecurity workforce, including a comparison of the different agencies and departments, and an analysis of the capacity of such agencies and departments to meet those needs;

(2) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide cybersecurity professionals with those skills sought by the Federal Government and the private sector, and a description of how successful programs are engaging the talents of females and individuals identified in section 33 or 34 of the Science and Engineer-

ing Equal Opportunities Act (42 U.S.C. 1885a or 1885b);

(3) an examination of the effectiveness of the National Centers of Academic Excellence in Information Assurance Education, the Centers of Academic Excellence in Research, and the Federal Cyber Scholarship for Service programs in promoting higher education and research in cybersecurity and information assurance and in producing a growing number of professionals with the necessary cybersecurity and information assurance expertise;

(4) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibilities; and

(5) recommendations for Federal policies to ensure an adequate, well-trained Federal cybersecurity workforce.

SEC. 108. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE.

(a) ESTABLISHMENT OF UNIVERSITY-INDUSTRY TASK FORCE.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall convene a task force to ex-

plore mechanisms for carrying out collaborative research and development activities for cybersecurity through a consortium or other appropriate entity with participants from institutions of higher education and industry.

(b) FUNCTIONS.—The task force shall—

(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration;

(3) define the roles and responsibilities for the participants from institutions of higher education and industry in such entity;

(4) propose guidelines for assigning intellectual property rights, for the transfer of research and development results to the private sector; and

(5) make recommendations for how such entity could be funded from Federal, State, and nongovernmental sources.

(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education, including minority-serving institutions and community colleges, and from industry with knowledge and expertise in cybersecurity.

(d) REPORT.—Not later than 12 months after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall transmit to the Congress a report describing the findings and recommendations of the task force.

SEC. 109. CYBERSECURITY CHECKLIST DEVELOPMENT AND DISSEMINATION.

Section 8(c) of the Cyber Security Research and Development Act (15 U.S.C. 7406(c)) is amended to read as follows:

"(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

"(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop or identify and revise or adapt as necessary, checklists, configuration profiles, and deployment

recommendations for products and protocols that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government.

"(2) PRIORITIES FOR DEVELOPMENT.—The Director of the National Institute of Standards and Technology shall establish priorities for the development of checklists under this subsection. Such priorities may be based on the security risks associated with the use of each system, the number of agencies that use a particular system, the usefulness of the checklist to Federal agencies that are users or potential users of the system, or such other factors as the Director determines to be appropriate.

"(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the requirements of paragraph (1) any computer hardware or software system for which the Director determines that the development of a checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a checklist for the system.

"(4) AUTOMATION SPECIFICATIONS.—The Director of the National Institute of Standards and Technology shall develop automated security specifications (such as the Security Content Automation Protocol) with respect to checklist content and associated security related data.

"(5) DISSEMINATION OF CHECKLISTS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any product developed or identified under the National Checklist Program for any information system, including the Security Content Automation Protocol and other automated security specifications.

"(6) AGENCY USE REQUIREMENTS.—The development of a checklist under paragraph (1) for a computer hardware or software system does not—

"(A) require any Federal agency to select the specific settings or options recommended by the checklist for the system;

"(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

"(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

"(D) preclude any Federal agency from procuring or deploying other computer hardware or software systems for which no such checklist has been developed or identified under paragraph (1).".

SEC. 110. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY RESEARCH AND DEVELOPMENT.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by redesignating subsection (e) as subsection (f), and by inserting after subsection (d) the following:

"(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall—

"(1) conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies and that is amenable to implementation within a wide variety of existing and emerging computing environments;

"(2) carry out research associated with improving the security of information systems and networks;

"(3) carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks; and

"(4) carry out research associated with improving security of industrial control systems.".

TITLE II—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

SEC. 201. DEFINITIONS.

In this title:

(1) DIRECTOR.—The term "Director" means the Director of the National Institute of Standards and Technology.

(2) INSTITUTE.—The term "Institute" means the National Institute of Standards and Technology.

SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

The Director, in coordination with appropriate Federal authorities, shall—

(1) ensure coordination of United States Government representation in the international develop-

ment of technical standards related to cybersecurity; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to the Congress a proactive plan to engage international standards bodies with respect to the development of technical standards related to cybersecurity.

SEC. 203. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION.

(a) PROGRAM.—The Director, in collaboration with relevant Federal agencies, industry, educational institutions, and other organizations, shall maintain a cybersecurity awareness and education program to increase public awareness of cybersecurity risks, consequences, and best practices through—

(1) the widespread dissemination of cybersecurity technical standards and best practices identified by the Institute; and

(2) efforts to make cybersecurity technical standards and best practices usable by individuals, small to medium-sized businesses, State, local, and tribal governments, and educational institutions.

(b) MANUFACTURING EXTENSION PARTNERSHIP.—The Director shall, to the extent appropriate, implement subsection (a) through the Manufacturing Extension Part-

nership program under section 25 of the National Institute of Standards and Technology Act (15 U.S.C. 278k).

(c) REPORT TO CONGRESS.—Not later than 90 days after the date of enactment of this Act, the Director shall transmit to the Congress a report containing a strategy for implementation of this section.

SEC. 204. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns, to—

(1) improve interoperability among identity management technologies;

(2) strengthen authentication methods of identity management systems;

(3) improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) improve the usability of identity management systems.

○

SECTION-BY-SECTION ANALYSIS OF H.R. 2096,
CYBERSECURITY ENHANCEMENT ACT OF 2011

Title I—Research And Development

Sec. 101. Definitions

Defines the terms National Coordination Office and Program in the title.

SEC. 102. Findings

Describes the findings of this title.

Sec. 103. Cybersecurity Strategic R&D Plan

Requires the agencies to develop, update and implement a strategic plan for cybersecurity research and development (R&D). Requires that the strategic plan be based on an assessment of cybersecurity risk, that it specify and prioritize near-term, mid-term and long-term research objectives and that it describe how the near-term objectives complement R&D occurring in the private sector.

Requires the agencies to solicit input from an advisory Committee and outside stakeholders in the development of the strategic plan. Additionally, requires the agencies to describe how they will promote innovation, foster technology transfer, and maintain a national infrastructure for the development of secure, reliable, and resilient networking and information technology systems.

Requires the development of an implementation roadmap that specifies the role of each agency and the level of funding needed to meet each of the research objectives outlined in the strategic plan.

Sec. 104. Social And Behavioral Research In Cybersecurity

Requires the National Science Foundation (NSF) to support research on the social and behavioral aspects of cybersecurity as part of its total cybersecurity research portfolio.

Sec. 105. NSF Cybersecurity R&D Programs

Reauthorizes the cybersecurity research program at the NSF and includes identity management as one of the research areas supported.

Reauthorizes programs at NSF that provide funding for capacity building grants, graduate student fellowships, graduate student traineeships and research centers in cybersecurity.

Repeals NSF cybersecurity faculty development traineeship program.

Sec. 106. Federal Cyber Scholarship For Service Program

Authorizes the cybersecurity scholarship for service program at NSF. The program provides grants to institutions of higher education for the award of scholarships to students pursuing undergraduate and graduate degrees in cybersecurity fields and requires an additional year of service over the number of years for which the scholarship was received.

The program also provides capacity building grants to institutions of higher education, supporting such activities as faculty professional development and the development of cybersecurity-related curricula and courses.

Sec. 107. Cybersecurity Workforce Assessment

Requires the President to issue a report assessing the current and future cybersecurity workforce needs of the federal government, including a comparison of the skills sought by Federal agencies and the private sector; an examination of the supply of cybersecurity talent and the capacity of institutions of higher education to produce cybersecruity professionals; and the identification of any barriers to the recruitment and hiring of cybersecurity professionals.

Sec. 108. Cybersecurity University-Industry Task Force

Establishes a university-industry task force to explore mechanisms and models for carrying out public-private research partnerships in the area of cybersecurity.

Sec. 109. Cybersecurity Checklist And Dissemination

Updates NIST's authority for the National Checklist Program (NCP) which provides detailed guidance on setting the security configuration of operating systems and applications for the federal government, and requires NIST to develop automated security specifications with respect to checklist content.

Sec. 110. NIST Cybersecurity R&D

Amends the National Institute of Standards and Technology Act to codify NIST cybersecurity research and development activities; NIST is authorized to develop a unifying and standardized identity, privilege, and access control management framework and to conduct research related to improving the security of information and networked systems, including the security of industrial control systems.

TITLE II—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

Sec. 201. Definitions

Defines the Terms Director and Institute in the title.

Sec. 202. International Cybersecurity Technical Standards

Requires NIST to develop and implement a plan to ensure a coordinated United States Government representation in international cybersecurity technical standards development. This plan is due to Congress no later than one year after enactment.

Sec. 203. Promoting Cybersecurity Awareness And Education

Requires NIST to maintain a cybersecurity awareness and education program and to deliver a plan to Congress within 90 days describing the implementation of this program. Requires the program to be aimed at disseminating cybersecurity best practices and standards and include how NIST will make these usable by individuals, small business, state and local governments, and educational institutions. Requires the plan to include how NIST can utilize established Manufacturing Extension Partnership networks to have cybersecurity information readily available to small manufacturing companies.

Sec. 204. Identity Management Research And Development

Requires NIST to continue research and development programs to improve identity management systems.

AMENDMENTS

AMENDMENT TO H.R. 2096

OFFERED BY MR. MCCAUL OF TEXAS

Page 7, line 24, strike "user" through "structures" and insert "and user motivations".

Page 22, after line 15, insert the following new subsections:

(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.

Page 22, line 16, through page 25, line 8, amend section 109 to read as follows:

SEC. 109. CYBERSECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.

Section 8(c) of the Cyber Security Research and Development Act (15 U.S.C. 7406(c)) is amended to read as follows:

"(c) SECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.—

"(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall

develop, and revise as necessary, security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government in order to enable standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security within the Federal Government.

"(2) PRIORITIES FOR DEVELOPMENT.—The Director of the National Institute of Standards and Technology shall establish priorities for the development of standards, reference materials, and checklists under this subsection on the basis of—

"(A) the security risks associated with the use of the system;

"(B) the number of agencies that use a particular system or security tool;

"(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

"(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

"(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

"(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a standard, reference material, or checklist for the system.

"(4) DISSEMINATION OF STANDARDS AND RELATED MATERIALS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

"(5) AGENCY USE REQUIREMENTS.—The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

"(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or checklist for the system;

"(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

"(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

"(D) preclude any Federal agency from procuring or deploying other information technology hardware or software systems for which no such standard, reference material, or checklist has been developed or identified under paragraph (1).".

Page 26, line 19, through page 27, line 7, amend section 202 to read as follows:

SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to the Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities specified in subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

Page 27, line 8, through page 28, line 6, amend section 203 to read as follows:

SEC. 203. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION.

(a) PROGRAM.—The Director, in collaboration with relevant Federal agencies, industry, educational institutions, and other organizations, shall continue to coordinate a cybersecurity awareness and education program to in-

crease knowledge, skills, and awareness of cybersecurity risks, consequences, and best practices through—

(1) the widespread dissemination of cybersecurity technical standards and best practices identified by the Institute; and

(2) efforts to make cybersecurity technical standards and best practices usable by individuals, small to medium-sized businesses, State, local, and tribal governments, and educational institutions.

(b) STRATEGIC PLAN.—The Director shall, in cooperation with relevant Federal agencies and other stakeholders, develop and implement a strategic plan to guide Federal programs and activities in support of a comprehensive cybersecurity awareness and education program as described under subsection (a).

(c) REPORT TO CONGRESS.—Not later than 1 year after the date of enactment of this Act and every 5 years thereafter, the Director shall transmit the strategic plan required under subsection (b) to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

At the end of the bill, insert the following new section:

SEC. 205. AUTHORIZATIONS.

No additional funds are authorized to carry out this title and the amendments made by this title or to carry out the amendments made by sections 109 and 110 of this Act. This title and the amendments made by this title and the amendments made by sections 109 and 110 of this Act shall be carried out using amounts otherwise authorized or appropriated.

☒

F:\M12\MCNERN\MCNERN_025.XML

AMENDMENT

OFFERED BY MR. MCNERNEY OF CALIFORNIA TO THE AMENDMENT OFFERED BY MR. MCCAUL OF TEXAS

Page 5, line 21, insert "National Laboratories," after "educational institutions,".

☒

Withdrawn

F:\M12\JOHNTE\JOHNTE_040.XML

#3

AMENDMENT

OFFERED BY MS. EDDIE BERNICE JOHNSON OF TEXAS TO THE AMENDMENT OFFERED BY MR. MCCAUL OF TEXAS

Page 6, line 5, strike "and".

Page 6, line 9, strike the period and insert a semicolon.

Page 6, after line 9, insert the following new paragraphs:

(3) increasing public awareness of cybersecurity risks, consequences, and best practices;

(4) improving the state of formal cybersecurity programs and activities at all education levels;

(5) ensuring that Federal agencies can attract, recruit, and retain qualified cybersecurity professionals; and

(6) improving the skills, training, and professional development of the Federal cybersecurity workforce.

☒

F:\M12\LUJAN\LUJAN_030.XML

AMENDMENT TO H.R. 2096

OFFERED BY MR. LUJÁN OF NEW MEXICO

Page 5, line 6, insert ", including consumer privacy," after "and trustworthiness".

AMENDMENT TO H.R. 2096

OFFERED BY MR. LUJÁN OF NEW MEXICO

Page 5, line 8, insert "rapid" after "will foster the".

Page 5, line 10, insert "timely" after "applications for the".

F:\M12\LUJAN\LUJAN_033.XML

AMENDMENT TO H.R. 2096

OFFERED BY MR. LUJÁN OF NEW MEXICO

Page 7, line 3, insert "National Laboratories," after "community colleges,".

☒

AMENDMENT TO H.R. 2096

OFFERED BY MR. SMITH OF TEXAS

Page 19, lines 21 and 22, strike "cybersecurity professionals with those skills sought by the Federal Government" and insert "current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities,".

Page 21, lines 1 and 2, strike "research and development" and insert "research, development, education, and training".

☒

AMENDMENT TO H.R. 2096

OFFERED BY MS. FUDGE OF OHIO

Page 20, line 11, insert ", including individuals from States or regions in which the unemployment rate exceeds the national average" after "assurance expertise".

☒

AMENDMENT TO H.R. 2096

OFFERED BY MR. CLARKE OF MICHIGAN

Page 25, lines 19 through 25, strike paragraph (1) (and redesignate the subsequent paragraphs accordingly).

Page 28, lines 7 through 22, amend section 204 to read as follows:

SEC. 204. IDENTITY MANAGEMENT TO IMPROVE CYBERSECURITY.

(a) RESEARCH AND DEVELOPMENT.—The Director shall continue a research program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns, to—

(1) improve interoperability among identity management technologies;

(2) strengthen authentication methods of identity management systems;

(3) improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) improve the usability of identity management systems.

(b) IDENTITY MANAGEMENT FRAMEWORK.—The Director, in collaboration with the private sector, is authorized to continue to facilitate the development of a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies that is amenable to implementation within a wide variety of existing and emerging computing environments.

(c) IMPLEMENTATION PLAN.—In carrying out the responsibilities under subsection (b), the Director shall coordinate and oversee the development of an implementation plan that identifies and assigns responsibility for near-term and long-term actions that the Federal Government will take to facilitate identity management technologies. The implementation plan may include activities that—

(1) leverage existing Federal efforts to implement near-term identity management solutions that align with the framework developed under subsection (b);

(2) remove barriers associated with private sector development of identity management technologies;

(3) ensure the privacy and protection of individuals within identity management systems; and

(4) promote the Federal Government as both a provider and consumer of identity management solutions.

☒

AMENDMENT TO H.R. 2096

OFFERED BY MR. LIPINSKI OF ILLINOIS

Page 27, after line 7, insert the following new section (and redesignate the subsequent sections accordingly):

SEC. 203. CLOUD COMPUTING STRATEGY.

(a) IN GENERAL.—The Director, in collaboration with the Federal CIO Council, and in consultation with other relevant Federal agencies and stakeholders from the private sector, shall continue to develop and implement a comprehensive strategy for the use and broad adoption of cloud computing services by the Federal Government.

(b) ACTIVITIES.—In carrying out the strategy developed under subsection (a), the Director shall give consideration to activities that—

(1) accelerate the development of standards that address interoperability and portability of cloud computing services;

(2) support the development of conformance test systems; and

(3) address appropriate security frameworks and reference materials for use by Federal agencies

to address their security and privacy requirements, including—

(A) the physical security of cloud computing data centers and the data stored in such centers; and

(B) accessibility of the data stored in cloud computing data centers.

☒

AMENDMENT TO H.R. 2096

OFFERED BY MR. WU OF OREGON

Page 27, after line 7, insert the following new section (and redesignate the subsequent sections accordingly):

SEC. 203. CYBERSECURITY STANDARDS COLLABORATION.

(a) IN GENERAL.—The Director is authorized to convene representatives of the private sector and other relevant stakeholders, including consumer groups, to collaborate on the development of consensus standards, guidelines, best practices, and voluntary codes of conduct related to information technology security for use by private sector entities that provide the following functions and services:

(1) Provision of information services and content.

(2) Facilitation of the wide variety of transactional services available through the Internet as an intermediary.

(3) Storage and hosting of publicly accessible content.

(4) Support of users' access to content or transaction activities, including application, browser, social network, and search providers.

(b) COORDINATION.—In carrying out the activities described in subsection (a), the Director shall coordinate with other relevant Federal agencies.

☒

AMENDMENT TO H.R. 2096

OFFERED BY MR. WU OF OREGON

Page 28, after line 6, insert the following new section (and redesignate the subsequent section accordingly):

SEC. 204. ASSESSMENT OF THE ROLE OF COMMUNITY COLLEGES IN CYBERSECURITY EDUCATION.

(a) IN GENERAL.—As part of the program described in section 203, the Director shall carry out an assessment of community colleges and cybersecurity education. The assessment shall include—

(1) a description of the current role of community colleges in cybersecurity education and the development of a skilled cybersecurity workforce;

(2) an identification of best practices used by community colleges to strengthen cybersecurity education and develop a skilled cybersecurity workforce; and

(3) recommendations on steps the Federal Government could take to improve or bolster the role of community colleges in cybersecurity education and the development of a skilled cybersecurity workforce.

(b) TIMELINE.—Not later than 1 year after the date of enactment of this Act, the Director shall submit the

assessment carried out under subsection (a) to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

(c) COORDINATION WITH OTHER RELEVANT AGENCIES.—In carrying out the assessment, the Director shall coordinate with other relevant Federal agencies involved in cybersecurity awareness and education, including the agencies that participate in the Networking and Information Technology Research and Development program as established under the High-Performance Computing Act of 1991 (15 U.S.C. 5511).

F:\TB\SC\CYBER11_001.XML

AMENDMENT TO H.R. 2096
OFFERED BY TONKO

At the end of the bill, insert the following new title:

TITLE III—LIMITATIONS

SEC. 301. LIMITATION ON AUTHORIZATIONS.

(a) OSTP.—For any fiscal year, the Director of the Office of Science and Technology Policy shall not be required to carry out section 108 of this Act unless the amount appropriated for the Office of Science and Technology Policy for that fiscal year is equal to or greater than the amount appropriated for the Office of Science and Technology Policy under the Department of Defense and Full-Year Continuing Appropriations Act, 2011 (Public Law 112–10).

(b) NIST.—For any fiscal year, the Director of the National Institute of Standards and Technology shall not be required to carry out section 20(e)(1) of the National Institute of Standards and Technology Act as amended by section 110 of this Act, and sections 202 and 203 of this Act unless the amount appropriated for the National Institute of Standards and Technology for that fiscal year is equal to or greater than the amount appropriated for the National Institute of Standards and Technology under

the Department of Defense and Full-Year Continuing Appropriations Act, 2011 (Public Law 112–10).

☒

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
Full Committee Markup
July 21, 2011

AMENDMENT ROSTER

H. R. 2096, the "Cybersecurity Enhancement Act of 2011"

No.	Amendment	Summary	Results
1	Mr. McCaul/Lipinski (024)	Makes minor clarifications to the Cybersecurity University-Industry Task Force section and technical changes to the bill; updates several provisions specific to the NIST activities in cybersecurity; includes language clarifying that no additional funds are authorized for NIST activities in the bill.	Agreed to by Voice Vote
2	Amendment Offered by Mr. McNerney (025) To McCaul Amendment (024)	Adds "National Laboratories" to the list of stakeholders with which the Director of NIST shall continue to coordinate a cybersecurity education and awareness program (sec. 203).	Agreed to by Voice Vote
3	REVISED Amendment Offered by Ms. Johnson (040) To McCaul Amendment (024)	Amends manager's amendment to expand the responsibilities of NIST's education and awareness program beyond their technical standards and best practices expertise to include a focus on improving formal cybersecurity programs and activities at all education levels, Federal workforce preparation, and public awareness, among other things.	Withdrawn
4	Mr. Lujan (030)	Amends the strategic plan in Section 103 to ensure it describes how the program will include technologies to protect consumer privacy.	En Bloc Amendment (1 of 6) Agreed to by Unanimous Consent
5	Mr. Lujan (032)	Amends the strategic plan to ensure that it is focused on how the program can ensure the "rapid" transfer of results from cybersecurity research and development and a "timely" benefit to society.	En Bloc Amendment (2 of 6) Agreed to by Unanimous Consent

6	Mr. Lujan (033)	Adds "National Laboratories" to the list of stakeholders that the agencies should solicit advice and recommendations from in the development of the strategic plan.	En Bloc Amendment (3 of 6) Agreed to by Unanimous Consent
7	Mr. Smith (042)	Adds language to the workforce assessment section to require review of the ability of universities to provide training and education in critical skills on cybersecurity; changes the focus of the cybersecurity task force to require the task force to explore mechanisms for "education and training" on cybersecurity as well as research and development.	En Bloc Amendment (4 of 6) Agreed to by Unanimous Consent
8	Ms. Fudge (027)	Requires the workforce assessment as it reviews the effectiveness of certain government programs in producing cybersecurity professionals to include areas with high unemployment .	En Bloc Amendment (5 of 6) Agreed to by Unanimous Consent
9	Mr. Clarke (CYBER11_003)	Strikes a research provision currently included in section 110 and inserts it into section 204; further builds upon existing provisions of section 204 to include the development of an implementation plan for the Federal government to provide and use identity management technologies.	Not Agreed to by Voice Vote
10	Mr. Lipinski (032)	Directs NIST to continue to develop and implement a comprehensive strategy for the use and adoption of cloud computing services by the Federal government.	En Bloc Amendment (6 of 6) Agreed to by Unanimous Consent
11	Mr. Wu (020)	Adds a new section providing NIST the authority to convene stakeholders within the information services sectors (e.g. content, storage, internet transactions) in order to develop consensus standards and voluntary codes of conduct for information security.	Withdrawn
12	Mr. Wu (019)	Requires NIST as part of the cybersecurity education and awareness program in section 203 to carry out an assessment of community colleges role in cybersecurity education and the development of a skilled cybersecurity workforce.	Withdrawn

13	Mr. Tonko (CYBER11_001)	The Director of the Office of Science and Technology Policy (OSTP) is not required to carry out the activities of the Cybersecurity University-Industry Task Force (sec. 108) unless the appropriation for OSTP for any fiscal year is equal or higher to FY11 appropriations. The same limitation is also included for the Director of NIST to carry out certain cybersecurity activities in research and development (sec. 110), international cybersecurity standards (sec. 202), and education and awareness (sec. 203).	Not Agreed to by a roll call vote of 13 Yeas and 17 Noes

Appendix II:

Submitted Statements in Support of Amendments to H.R. 2096

SUBMITTED STATEMENT BY REPRESENTATIVE WU (AMENDMENT 20 TO H.R. 2096)

Thank you, Mr. Chairman.

My amendment would give authority to the Director of NIST to convene representatives of the private sector and other relevant stakeholders, including consumer groups, to collaborate on the development of consensus standards, guidelines, best practices, and voluntary codes of conduct related to information technology security for use by certain private sector entities.

In June, after extensive public input, the Internet Policy Task Force at the Department of Commerce released a green paper entitled "Cybersecurity, Innovation, and the Internet Economy."

The paper addresses the growing economic importance of cybersecurity and of preserving consumer trust in the Internet, and it includes a handful of recommendations on ways to strengthen cybersecurity for companies that specifically rely on the Internet to do business.

One of the recommendations in that report was for the Department of Commerce, through NIST, to convene businesses in the Internet and information innovation sector, or the so-called I3S, to facilitate the development of voluntary consensus codes of conduct (including technical standards, practices, and guidelines) for cybersecurity.

The report makes clear that NIST's involvement would be limited to assisting industry in those areas where collective action among private sector stakeholders is lacking and where gaps currently exist.

SUBMITTED STATEMENT BY REPRESENTATIVE WU (AMENDMENT 24 TO H.R. 2096)

Thank you, Mr. Chairman.

My amendment is intended to highlight the unique and important role that community colleges can—and should—play in cybersecurity education and the training of cybersecurity professionals.

In addition to serving on this committee, I serve as a co-chair of the Congressional Community College Caucus. Community colleges are oftentimes best suited to educate and train students in order to meet the employment needs of local businesses and government.

Moreover, community colleges play a critical role in educating our science and technology workforce.

In fact, the American Association of Community Colleges estimates that "44 percent of students who receive baccalaureates or master's degrees in STEM fields attended a community college at some point in their careers."

My amendment is simple. It requires the Director of NIST to carry out an assessment of community colleges and cybersecurity education, including:

- a description of the current role of community colleges in cybersecurity education and the development of a skilled cybersecurity workforce;
- an identification of best practices; and
- recommendations on steps the federal government can take to improve or bolster the role of community colleges in this space.

As we are all aware, NIST has been charged with coordinating and overseeing the interagency National Initiative on Cybersecurity Education (NICE), which is a broad initiative focused on several critical aspects of cybersecurity education and the development of a skilled cybersecurity workforce.

Although this initiative is not clearly spelled out in the underlying bill, it is my intent that the Director of NIST be in charge of this assessment in his capacity as the coordinator and overseer of NICE.

It is my full expectation that the Director will coordinate and oversee the other agencies that are part of the initiative in the development of this assessment, and not carry out this assessment on his own.

I think there is value to having the participation of all of the agencies involved in cybersecurity education in the assessment, and NICE seems like an appropriate place to ensure that this will happen.

I am aware that the workforce assessment under Section 107 includes an examination of the capacity of institutions of higher education, including community colleges, to provide cybersecurity professionals with the skills sought by the federal government and the private sector.

This is certainly important and I support it. However, I note that in Section 107, community colleges are but one small mention in a small piece of a much larger workforce assessment.

For all intents and purposes, in Section 107, community colleges are no more than an afterthought.I believe that community colleges deserve a much more thorough and comprehensive look and that it is important that we pull them out and give them the respect they deserve.

There is no doubt that community colleges have an important role to play in training future cybersecurity professionals.

Not only are they in a position to train students just entering the workforce to work in the cybersecurity field, but they can also play a unique role in re-training people to transition into a career in cybersecurity.

We often hear about the need for more skilled cybersecurity professionals. At the same time, in this tough economy, far too many people are out of work and looking for jobs.

If community colleges can re-train technical workers-for example, NASA workers who are out of work now that the shuttle program is wrapping up-and provide them with the skills they need to transition into the cybersecurity field and, at the same time, help us meet our need for new cybersecurity professionals—then that's an opportunity we ought to be exploring and pursuing.

My amendment is also intended to fill a gap that was left between the bill from last Congress and the bill as introduced this Congress.

In the last Congress, an amendment was offered and accepted on the House floor requiring a study on the role of community colleges in cybersecurity education. Unfortunately, for reasons I don't fully understand, that provision was taken out of the bill this Congress before introduction.

My amendment will ensure that the bill gives adequate consideration to the role that community colleges can play in cybersecurity education, similar to the bill that passed the House last Congress.

This is a good amendment, and I urge its adoption.

○